COMITE DE TRANSPARENCIA

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

2026

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

COMITE DE TRANSPARENCIA

UNIDAD_TRANSPARENCIA@CONGRESOCHIAPAS.GOB.MX
WWW.TRANSPARENCIA.CONGRESOCHIAPAS.GOB.MX

Tabla de contenido

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 numeral 5º fracción XVI de la Constitución Política del Estado Libre y Soberano de Chiapas; asimismo, los servidores públicos que tengan acceso a datos personales están obligados a conocer y aplicar las medidas que resulten necesarias para salvaguardar los mismos y garantizar la privacidad de las personas de que se traten, desde la obtención hasta la eliminación de dichos datos.

En ese sentido, resultan de gran relevancia las reformas y adiciones que en la materia se han realizado a nuestra Constitución Política de los Estados Unidos Mexicanos, para salvaguardar este derecho humano; mismas que dieron pauta para que el 26 de enero de 2017, se publicara en el Diario Oficial de la Federación, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, cuyo objetivo conforme al artículo 1º., párrafo tercero de la misma, es establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal, estatal y municipal.

Es por ello que está LXIX Legislatura del Honorable Congreso del Estado de Chiapas, a fin de dar cumplimiento a las obligaciones estipuladas en la nueva reforma en los artículos 29 y 30 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; esto para poder elaborar el Documento de Seguridad de Datos Personales de esta Sede legislativa, el cual contempla el ciclo PHVA (Planear-Hacer-Verificar y Actuar); para ello se inició con un diagnóstico a través de un

inventario de datos personales, se conocieron las funciones y obligaciones de las personas que tratan datos personales, también se realizó el análisis de brecha de las medidas de seguridad y el análisis de riesgo de vulneraciones, así también se generaron las medidas de seguridad necesarias, se realizó una carta de confidencialidad, se planteó un programa de capacitación y finalmente la verificación o evaluación de las medidas de seguridad, para poder actualizar y mejorar paulatinamente.

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

Es relevante mencionar que el contenido del documento de seguridad se realizó con la colaboración de las áreas que conforman este H. Congreso del Estado y que manifestaron tratar datos personales, en coordinación con la Unidad de Transparencia; conforme a las disposiciones normativas, a efecto de visibilizar las acciones actuales y planear las futuras para el adecuado tratamiento de los datos personales.

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 ADMINISTRATIVAS**: A las Coordinaciones, Direcciones, Unidades y demás áreas que integran la estructura orgánica del Congreso, que cuentan o puedan contar, dar tratamiento y ser responsables o encargadas 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 administrativas distintas dentro del H. Congreso del Estado de Chiapas.
- **DATOS PERSONALES:** Cualquier información concerniente a una persona física identificada o identificable.

- **PERSONA 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, género y preferencia sexual.
- **DERECHOS ARCO**: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.
- **ENLACE:** La persona designada por el titular de las áreas responsables para fungir como responsable entre el área y la Unidad de Transparencia, con la finalidad de construir, asesorar e informar, las acciones en materia de protección de datos personales.
- **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.
- **AUTORIDAD GARANTE:** A la Contraloría Interna del Congreso del Estado, en términos del artículo 34, fracción II, de la Ley de Transparencia y Acceso a la información pública del Estado de Chiapas.
- **MEDIDAS DE SEGURIDAD ADMINISTRATIVAS:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado

seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

- **MEDIDAS DE SEGURIDAD FÍSICAS:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.
- **MEDIDAS DE SEGURIDAD TÉCNICAS:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. Responsable de área: Titulares de las unidades administrativas que integran el H. Congreso, que manifestaron tratar datos personales.
- **RIESGO:** Combinación de la probabilidad de un evento y su consecuencia desfavorable.
- **SUJETO RESPONSABLE:** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Ayuntamientos, Órganos Constitucionales Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, en este caso el H. Congreso del Estado de Chiapas.
- **TITULAR**: Persona física a quien corresponden los datos personales.
- **TRANSFERENCIAS:** Toda comunicación de datos personales que se realiza a persona o dependencia distinta del H. Congreso del Estado de Chiapas, ya sea dentro o fuera del territorio mexicano.
- **TRATAMIENTO**: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.
- **USUARIO:** La persona que, por sus actividades laborales y atribuciones legales, tenga acceso a los datos personales.

- **VERIFICACIÓN:** Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este documento.
- **VULNERABILIDAD:** Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.
- **CARTA DE CONFIDENCIALIDAD:** contrato legal que obliga a una o ambas partes a no divulgar información sensible o estratégica de la Sede Legislativa

FUNDAMENTO LEGAL DE DOCUMENTO DE SEGURIDAD

- **Constitución Política de los Estados Unidos Mexicanos en sus artículos 6º, Inciso A y 16 párrafo segundo.**
- **Constitución Política del Estado Libre y Soberano de Chiapas, en sus artículos 3º y 5º fracción XVI.**
- **Ley de Desarrollo Constitucional del Congreso del Estado de Chiapas en sus artículos 75, 76 y 77**
- **Ley de Protección de Dato Personales en Posesión de Sujetos Obligados del Estado de Chiapas, en sus artículos 29 y 30.**
- **Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales del Honorable Congreso del Estado de Chiapas, en su artículo 35, 36 y demás disposiciones vigentes aplicables.**

1. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTOS

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 el área administrativa que integran el H. Congreso del Estado de Chiapas, realizado con orden y precisión, en términos del artículo 29 fracción I de la Ley de Protección de Dato Personales en Posesión de Sujetos Obligados de Chiapas.

Para dar cumplimiento a los establecido en el artículo 29, fracción I de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, y para efecto de obtener un diagnóstico del conocimiento y tratamientos de datos personales, previa capacitación se elaboraron diversos formularios que fueron llenados por las distintas áreas administrativas, enfocándose en dos actividades:

1. Precisar que acción o procedimiento realizan y que tipo de datos personales son tratados por cada proceso
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 bien su destrucción. De acuerdo al análisis realizado de los distintos inventarios de datos personales, se desprendió que son 19 áreas las que manifestaron tratar datos personales, las cuales fueron enlistadas en el apartado 3 de este documento.

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 lso datos peronslaes de los titulares
Tipo de datos personales tratados	•Datos personales necesarios para que el sujeto obligado pueda dar atención al tratamiento. Se diferencia 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, explicigtas, y legitimas
Áreas y servicios 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, electronico 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 tratamientos de datos personales

2. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

Un aspecto de suma importancia que deriva de la protección de datos personales, es la de establecer las funciones y obligaciones de las personas servidoras públicas que tratan datos personales; en ese sentido, conforme a la información que la Unidad de Transparencia ha recabado, se tiene documentado cuales son las áreas administrativas y los nombres de las personas que están tratando datos personales conforme a las actividades o funciones que realizan diariamente. De esta forma, se da pleno cumplimiento al numeral 29, fracción II de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas.

Derivado de lo anterior y para dar cumplimiento, **en la siguiente tabla se puede observar el nombre del área, los procesos, la finalidad y los usuarios o servidores públicos que realizan los procesos.**

PROCESO, FINALIDAD Y USUARIO				
UNIDAD ADMINISTRATIVA	**ÁREAS**	**PROCESO**	**FINALIDAD DEL TRATRAMIENTO**	**USUARIOS DEL PROCESO**
JUNTA DE COORDINACIÓN POLÍTICA	PRESIDENCIA	Registro de personas que solicitan audiencia y programación de reuniones de traba	Consulta	Mtro. Christian de Jesús García Arce
		Videocámaras	Seguridad	
		Propuestas al pleno para la integración de las comisiones legislativas	Consulta	
	UNIDAD DE TESORERÍA	Alta de nómina de Diputados	Para pago	C. María de los Ángeles Pérez Jiménez
		Pago de Cheques		
		Pago de proveedores		
SECRETARÍA DE SERVICIOS ADMINISTRATIVOS	UNIDAD DE SERVICIOS DE RECURSOS HUMANOS	Contratación y alta de personal	No se cuentan	- Lic. Arminda Escobar Matuz

		Altas y bajas del IMSS	Para ser ingresados a los servicios de salud del IMSS	- Lic. Arminda Escobar Matuz
		Inscripción y Créditos INFONACOT	Para conocer a quienes se les aplicarán las deducciones. Para el resguardo de información de los trabajadores, contar con información para el trabajador	- Lic. Arminda Escobar Matuz
		Elaboración y dispersión de nomina	Elaboración de nómina y pago de salario de trabajadores	Lic. Arminda Escobar Matuz
		Inscripción y créditos al INFONAVIT	Movimientos de afiliación de INFONAVIT	Lic. Arminda Escobar Matuz
			Descuento por crédito INFONAVIT	
		Solicitudes de Información y Obligaciones de la Plataforma Nacional	Dar cumplimiento a las obligaciones de transparencia	Lic. Arminda Escobar Matuz
		Seguro de vida	Seguridad Social	- Lic. Arminda Escobar Matuz

		Elaboración de constancias	Declaración Anual	- Lic. Arminda Escobar Matuz
	UNIDAD DE RECURSOS MATERIALES	Directorio de proveedores	Para realizar acciones de cotizaciones, compras y/o adquisiciones con los proveedores	Lic. María Alejandra Gutiérrez Clemente
		Generación de Resguardos	Para control y resguardo de los bienes muebles del H. Congreso del Estado	
		Atención a requerimientos de los diputados	Atención a requerimientos de los diputados	
		Servicios Médicos y de Atención a los diputados y diputadas	Servicios de Salud	
	UNIDAD DE CONTABILIDAD Y CONTROL PRESUPUESTAL	Resguardo de información	Resguardar la información de manera digital	C.P. Carlos Alberto López Consospó
	UNIDAD DE PLANEACIÓN Y PRESUPUESTO	Integrar y Publicar formato de montos por ayudas y subsidios	Integrar y publicar trimestralmente formato de montos pagados	- C.P. Laura Lilia Arrevillaga Cano

			por ayudas y subsidios	
DIRECCIÓN DE COMUNICACIÓN SOCIAL	DIRECCIÓN DE COMUNICACIÓN SOCIAL	Servicios de Publicidad Cobertura de eventos y producción de material gráfico y audiovisual Proceso informativo para medios de comunicación Monitoreo de la síntesis informativa	Registro de personas que realizan la cobertura de las actividades legislativas	- Ing. Ricardo Espinoza Vera
CONTRALORÍA INTERNA Y AUTORIDAD GARANTE DEL PODER LEGISLATIVO	CONTRALORÍA INTERNA Y AUTORIDAD GARANTE DEL PODER LEGISLATIVO	Buzón de Sugerencias, Propuestas, Quejas y Denuncias Declaración patrimonial y de interés publico Seguro de Vida	Recibir y dar seguimientos Seguimiento para el cumplimiento - Datos de póliza SDV - Asignación de beneficiario	Lic. Mariana Guadalupe Domínguez López

			- Autorización del asegurado - Datos para póliza SDV	
		Acta-Entrega Recepción	Forman parte del contenido del Acta-Entrega Recepción en el apartado de identificación del servidor público	
		Procedimientos de Responsabilidad Administrativa	Tramite de expediciones	
		Registro de asistencia a cursos de capacitaciones, talleres y reuniones de trabajo	Comunicación efectiva	
COORDINACIÓN DE ATENCIÓN A MUNICIPIOS	COORDINACIÓN	Atender los Asuntos relacionados con los Municipios	La tramitación y solución de los asuntos planteados	
UNIDAD DE TRANSPARENCIA	ÁREA DE ACCESO A LA INFORMACIÓN PÚBLICA	Atención de solicitudes de Acceso a la información Pública y de Derechos ARCO	La tramitación y respuesta de las solicitudes	Lic. Rodolfo Ruíz Padilla

		Atención a denuncias de las obligaciones de Transparencia	Tramitación de los expedientes	
		Atención a requerimientos del Autoridad Garante	Brindar cumplimiento a los distintos requerimientos	
		Directorio de Enlaces (Capacitación reuniones de trabajo)	Comunicación efectiva	Lic. Rodolfo Ruiz Padilla
	ÁREA DE PROTECCIÓN DE DATOS PERSONALES	Atención a los requerimientos de verificación de la Autoridad Garante	Tramitación del procedimiento de verificación	C. Fernando Rubelin Pérez Briones
MESA DIRECTIVA	PRESIDENCIA	Programación de Reuniones de Trabajo con la Representante de la Mesa Directiva	Atención a los temas concernientes a la Presidencia de la Mesa Directiva	
		Registro de Atención al Público	Brindar atención a la ciudadanía	
SERVICIOS PARLAMENTARIOS	SECRETARÍA DE SERVICIOS PARLAMENTARIOS	Solicitudes de Desincorporaciones de Predios del patrimonio	Tramites de las solicitudes	Lic. Arlena Morales Morales

		municipal presentadas por los Ayuntamientos		
		Propuestas de Nombramientos de Servidores Públicos	Designación de servidores públicos	
INSTITUTO DE INVESTIGACIONES LEGISLATIVAS Y ESTUDIOS LEGISLATIVOS PARA LA IGUALDAD DE GÉNERO	INSTITUTO DE INVESTIGACIONES LEGISLATIVAS Y ESTUDIOS LEGISLATIVOS PARA LA IGUALDAD DE GÉNERO	Control de Oficios	Consulta	Lic. Deborah Cancino Alamilla Lic. Karina Díaz Flores
		Coordinación de visitas guiadas por orden de la Mesa Directiva	Consulta y estadísticas	
		Agenda Legislativa	Investigación	
		Investigaciones Legislativa	Trámites	
	BIBLIOTECA	Prestamos de Material Bibliográfico	-Control de acceso -Control de préstamos de libros -Control de equipo de cómputo	
		Registro de acceso y uso de los equipos de computo	Control de equipo de Cómputo	
	HEMEROTECA	Consulta a Diarios Locales	Registro de Usuarios	
	ARCHIVO HISTÓRICO	Brindar asesorías y capacitaciones al	Capacitación	

		personal del H. Congreso del Estado		
		Implementación de la clasificación archivística de la documentación en las áreas que integran el H. Congreso del Estado	Los datos personales recabados son utilizados únicamente para el acto o efecto para el cual son solicitados, posteriormente se eliminan	
		Préstamo de documentación para tramites de las áreas internas del H. Congreso del Estado	Registro de usuarios	
		Préstamo de documentación para consulta archivística	Registro de usuarios	
DIRECCIÓN DE ASUNTOS JURÍDICOS	DIRECCIÓN DE ASUNTOS JURÍDICOS	Actas administrativas	Trámite	Lic. Gustavo Fernández Díaz
		Contratos y Convenios	Consulta	
		Procesos Jurídicos	Trámite	

UNIDAD DE INFORMATICA	ÁREA DE DESARROLLO DE SISTEMAS	Credencialización oficial del H. Congreso del Estado de Chiapas	La elaboración de la credencialización	Ing. Gerardo Francisco Nájera Vázquez
		Directorio de Diputados	Registrar los directorios de los diputados	
	ÁREA DE SOPORTE TÉCNICO	Solicitudes de Servicios Web	Para dar trámite a las solicitudes	
		Solicitudes de servicio	Para dar trámites a las solicitudes	

3. ANÁLISIS DE RIESGOS Y DE BRECHA.

Con la finalidad de garantizar la seguridad de los datos personales, se debe implementar y fortalecer distintas acciones que fomenten la confidencialidad, la integridad y la disponibilidad de los mismos, para lograrlo, se debe tomar en cuenta la herramienta del análisis de riesgo.

El documento de seguridad describe y establece los criterios de evaluación y tratamiento de riesgos, esta herramienta resulta muy útil en los procesos de tratamiento de datos personales en posesión del Honorable Congreso del Estado.

El análisis de riesgo permite una adecuada toma de decisiones en relación a las acciones que deberán implementarse ante la vulneración de datos personales, de igual manera, permite de finir cual será el procedimiento o el método para evaluar y tratar los riesgos que se presenten en el futuro.

Así entonces y conforme a la normatividad, misma que señala, que es obligación de los sujetos obligados el determinar los riesgos existentes y la posibilidad de mitigarlos a través de un análisis cuantitativo, Sobre el impacto y la probabilidad de que una amenaza vulnere la seguridad, tanto en la información de

los datos personales, como en los recursos involucrados, lo que dará pauta a la implementación de medidas de seguridad.

Bajo esta premisa, para analizar los riesgos de los datos personales, que son objeto de tratamiento por el H. Congreso del Estado de Chiapas, se aplicó un instrumento para, clasificar los datos utilizados, a partir de la siguiente caracterización 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 una persona 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 nacimientos.

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

3). Académicos, se refiere a la trayectoria educativa, títulos, cedula profesional, certificado, reconocimientos y constancias.

4). Patrimoniales, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, cuentas bancarias, estadio de cuenta, clave interbancaria, bienes muebles, e inmuebles, los créditos las tarjetas de debido, 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 a un riesgo grave para éste como, por ejemplo, **datos de salud**, el **origen étnico** o **racial**, **ideológicos** (las creencias religiosas, filosóficas, afiliación político o

sindical, pertenencia a organizaciones religiosas o de la sociedad civil), **género y preferencia 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 voz u otros análogos); **correos electrónicos particulares** (Número de identificación personal (NIP), correos electrónicos, contraseñas, entre otros) y las **características físicas** (color de piel, color de iris, color de cabello, señas particulares, discapacidades, entre otros).

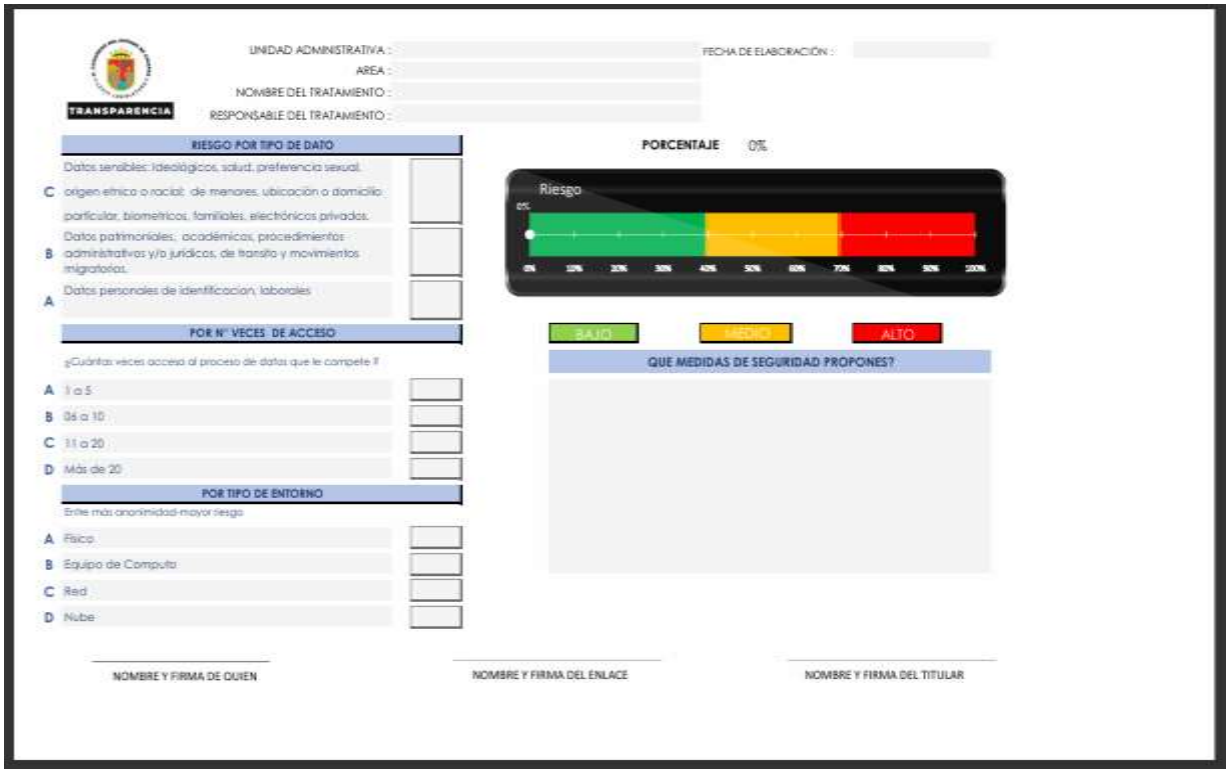
B) Metodología de Análisis de Riesgo

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 entrono 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 tratados, **B**, el número de veces que acceden, **C**, el tipo de entorno que son tratados, y el factor **n**, es el número de combinaciones posibles entre las mismas. En los rubros **A** y **C**, se pueden sumar uno o más tipos de datos, mientras que en el rubro **B**, solo se puede elegir uno; esto nos da la posibilidad de distintas combinaciones (**factorial n**) (**anexo 1**), las cuales nos dieron la oportunidad de determinar un porcentaje de valor cuantitativo a cada rubro **A**, **B** y **C**; dicho porcentaje se representó en la gráfica de calor (**anexo 3**), arrojando un porcentaje de riesgo latente.

Al primer rubro (**A**). Denominado riesgo por tipo de datos, y que a su vez se integra por **3** categorías de datos, se le asignó un porcentaje del **50%**; dividido entre los mismo; al segundo rubro (**B**), titulado riesgo por número de veces de acceso, que se integra por **4** categorías, se le asignó un porcentaje del **20%**, dividido entre los mismos, y al tercer rubro (**C**), denominado riesgo por tipo de entorno, que se integra por 4 categorías, se le asignó un porcentaje del **30%** dividido entre los mismos (**Anexo 3**). Está gráfico 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 ampliada consistió en un formato denominado **formulario de análisis de riesgo** (**anexo 2**), y una **gráfica de calor (anexo 3)**, en la que cada área representó. El nivel de riesgo de los tres parámetros antes escritos.

A.- **Riesgo por tipo de datos**

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

TIPOS DE DATOS	RIESGO INHERENTE	NIVEL DE RIESGO
Daros identificativos, laborales.	BAJO	A
Datos patrimoniales, académicos y 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 1. Riesgo por tipo de datos (verde bajo, ámbar medio, rojo alto)

Cabe señalar que los datos personales que son tratados en el H. congreso, son los siguientes:

- Datos identificados,
- Datos académicos,
- Datos laborales,
- Datos de familiares,
- Datos patrimoniales,
- Sensibles:
    1. De salud
    2. Ideológicos
    3. Características físicas

La tipología enunciada se retomó del plasmado en el inventario de datos personales, por los usuarios irresponsables 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 hacen 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 del grado de vulnerabilidad, es mayor cuando se accede más números 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 – 10 veces
- De 11 – 20 veces
- Más de 20 veces

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

ÓRGANOS DE GOBIERNO, UNIDADES ADMNISTRATIVAS Y ÁREAS	NO. DE VECES QUE ACCEDEN	
	DE 1 A 5	DE 6 A 10
JUNTA DE COORDINACIÓN POLÍTICA	**3***	
MESA DIRECTIVA	**2***	
SECRETARÍA DE SERVICIOS PARLAMENTARIOS Unidad de Archivo y Correspondencia	**1***	
Unidad de Trámites Legislativos	**1***	
SECRETARÍA DE SERVICIOS ADMINISTRATIVOS Unidad de Tesorería	**3***	
Unidad de Planeación y Presupuesto	**1***	
Unidad de Servicios de Recursos Humanos	**8***	
Unidad de Recursos Materiales	**3***	

Servicios Médicos y de Atención a los Diputados y Diputadas	**1***	
Unidad de Contabilidad y Control Presupuestal	**2***	
INSTITUTO DE INVESTIGACIONES LEGISLATIVAS Y ESTUDIOS LEGISLATIVOS PARA LA IGUALDAD DE GÉNERO	**4***	**1***
Departamento de Biblioteca	**1***	**2***
Departamento de Hemeroteca	**1***	
Área de Archivo Histórico	**5***	
DIRECCIÓN DE ASUNTO JURÍDICOS	**3***	
CONTRALORÍA INTERNA DEL PODER LEGISLATIVO	**5***	**1***
DIRECCIÓN DE COMUNICACIÓN SOCIAL	**2***	
UNIDAD DE TRANSPARENCIA Área de Acceso a la Información Pública	**4***	
Área de Protección de Datos Personales	**2***	
UNIDAD DE INFORMATICA Área de Desarrollo y Sistemas	**3***	*
Área de Soporte Técnico		1*
COORDINACIÓN DE ATENCIÓN A MUNICIPIOS	**1***	

*Número de procesos por área. **Cuadro 1. 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 al entorno desde los cuales se acceden desde a los datos personales, entre mayor sea 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 el entorno a que sucede 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 aprecian los entornos a que acceden las distintas áreas.

ÓRGANOS DE GOBIERNO, UNIDADES Y ÁREAS	TIPO DE ENTORNO			
	FÍSICO	PC	RED	NUBE
JUNTA DE COORDINACIÓN POLÍTICA				
Coordinación de Atención a Municipios				
SECRETARÍA DE SERVICIOS ADMINISTRATIVOS				
Unidad de Tesorería				
Unidad de Servicios de Recurso Humanos				
Unidad de Recursos Materiales y Servicios Generales				
Unidad de Contabilidad y Control Presupuestal				
Unidad de Planeación y Presupuesto				
DIRECCIÓN DE COMUNICACIÓN SOCIAL				
CONTRALORÍA INTERNA				
UNIDAD DE TRANSPARENCIA				
Áreas de Acceso a la Información Pública				
Área de Protección de Datos Personales				
MESA DIRECTIVA				

SECRETARÍA DE SERVICIOS PARLAMENTARIOS				
Unidad de los Archivos de Trámite				
Trámites Legislativos				
INSTITUTO DE INVESTIGACIONES LEGISLATIVAS Y ESTUDIOS LEGISLATIVOS PARA LA IGUALDAD DE GÉNERO				
Biblioteca				
Hemeroteca				
Archivo Histórico				
DIRECCIÓN DE ASUNTOS JURÍDICOS				
UNIDAD DE INFORMATICA				
Área de Desarrollo y Sistemas				
Área de Soporte Técnico				
TOTAL DE ÁREAS POR TIPO DE ENTORNO	**18**	**16**	**14**	**6**

Cuadro 2. Descripción de los tipos de entorno a los que acceden a las distintas áreas.

C). **Análisis de la información**

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

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

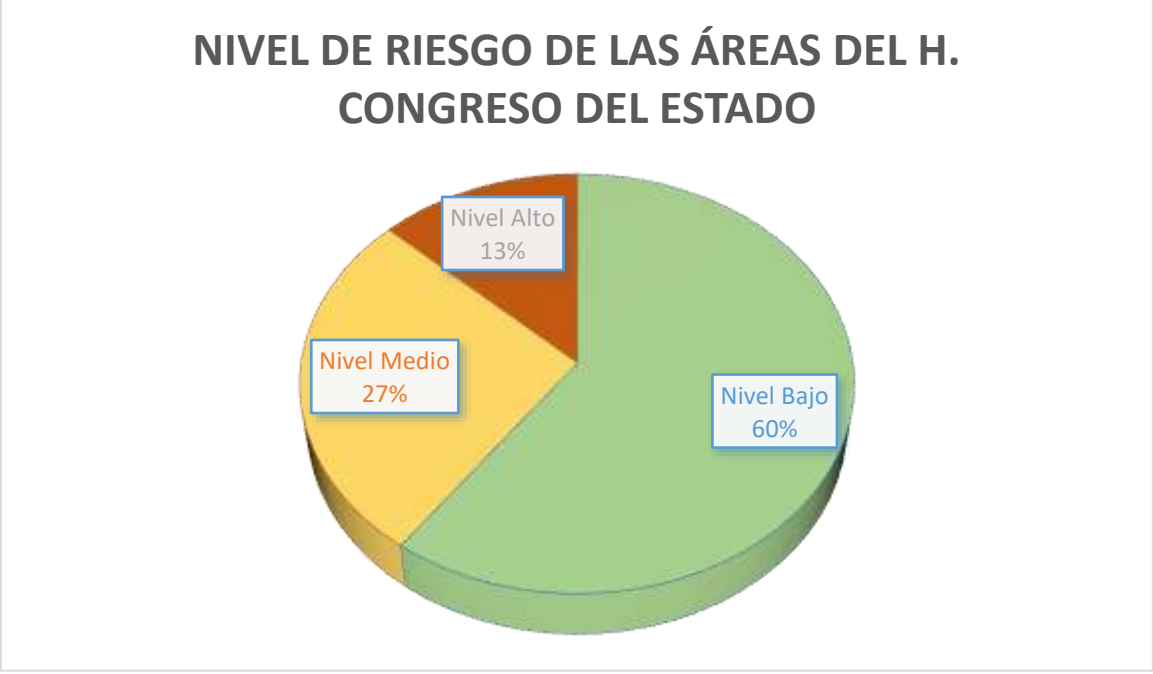
Contraloría con un proceso, esto implica que sus procesos relativos a la protección de datos personales, sean aplicados mayor atención y cuidado, con la intensión de garantizar que el derecho a la protección de datos personales se cumpla.

Para mayor comprensión se muestra a la siguiente tabla.

NIVEL DE RIESGO POR ÁREA Y NÚMERO DE PROCESOS					
NIVEL BAJO	POR ÁREA	NIVEL MEDIO	POR ÁREA	NIVEL ALTO	POR ÁREA
ARCHIVO HISTORICO	5	INFORMATICA	1	INFORMATICA	1
HEMEROTECA	1	TRANSPARENCIA	1	CONTRALORÍA DEL PODER LIGISLATIVO	2
BIBLIOTECA	2	CONTRALORÍA INTERNA DEL PODER LESGISLATIVO	4	DIRECCIÓN DE ASUNTOS JURÍDICOS	3
INFORMATICA	2	SERVICIOS DE RECURSOS HUMANOS	2	SERVICIOS DE RECURSOS HUMANOS	2
CONTABILIDAD Y CONTROL PRESUPUESTAL	1	PLANEACIÓN Y PRESUPUESTO	1	JUNTA DE COORDINACIÓN POLÍTICA	1
COMUNICACIÓN SOCIAL	4	INVESTIGACIONES LEGISLATIVAS	2		
PLANEACIÓN Y PRESUPUESTO	1	RECURSOS MATERIALES Y SERVICIOS GENERALES	3		1
INVESTIGACIONES LEGISLATIVAS Y ESTUDIOS LEGISLATIVOS PARA	4				

LA IGUAL DE GÉNERO					
TESORERÍA	3				
PARLAMENTARIOS	2				
SERVICIO DE RECURSOS HUMANOS	5				
TRANSPERENCIA	5				
JUNTA DE COORDINACIÓN POLÍTICA	2				
MESA DIRECTIVA	2				
COORDINACIÓN DE ATENCIÓN A MUNICIPIOS	1				
TOTAL DE PROCESOS					
	40		**13**		**10**

Cuadro 2. Descripción del semáforo de nivel de riesgo, que tienen los procesos de cada área



Cuadro 3. Representación gráfica del porcentaje de riesgo, conforme a los procesos que tratan las áreas del H. Congreso del Estado.

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

4. EL ANÁLISIS 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, está 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, con base en el Artículo 29 fracción IV de la Ley de Protección de Dato Personales en Posesión de Sujetos Obligados de Chiapas

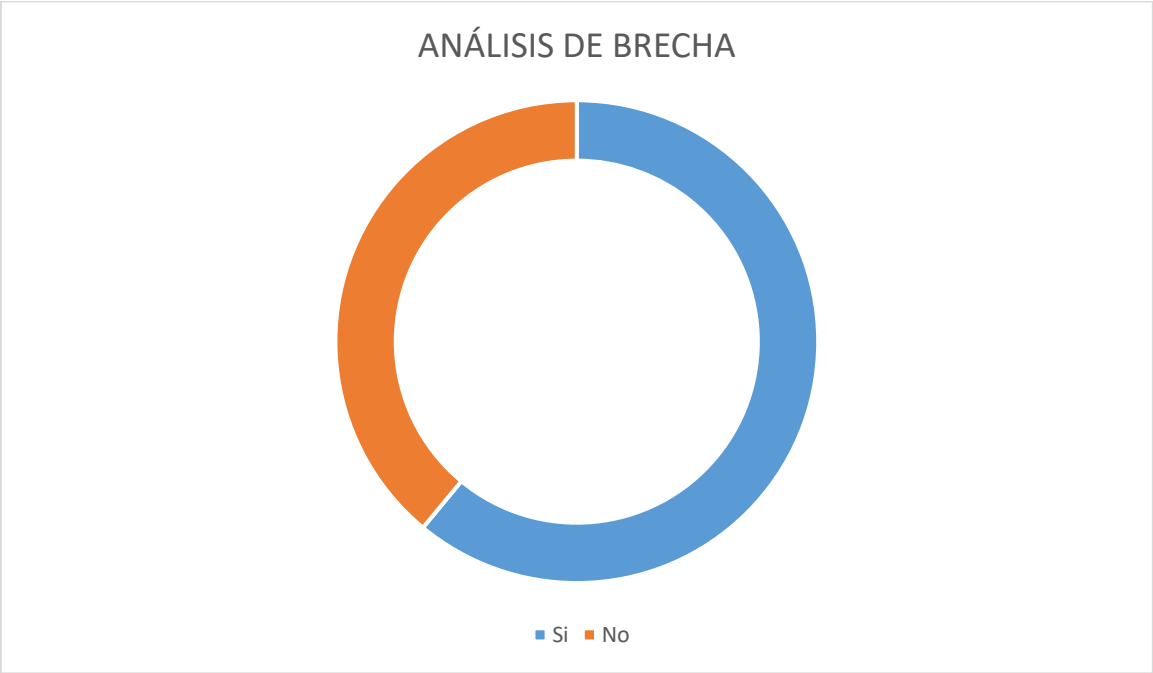
En esta tesitura, nuestra herramienta consistió en un formato denominado "Análisis de Brecha" (**anexo 4**), el cual fue llenado por los responsables de cada área de acuerdo a sus procesos en los que tratan de datos personales; este documento contiene una serie de medidas a manera de preguntas, para responder si se cuenta o no con ella y un campo más de observaciones; en este instrumento se consideraron 3 rubros a saber:

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

Del análisis realizado de las encuestas se concluyó qué, el 61.22% de las áreas manifestaron realizas 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 existente y faltante.



Cuadro 4. 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, sustentando en la normatividad vigente.

5. EL PLAN DE TRABAJO

Son acciones que se van a terminar con cada área o unidad administrativa correspondiente para adoptar un plan de trabajo que permita la implementación de medidas de seguridad faltantes para el cumplimiento cotidiano de las políticas de gestión y tratamiento de datos personales de este poder legislativo.

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

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

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

Lo anterior sustentado por el Artículo 29 fracción V de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas.

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

Una manera de mejora continua es a través del monitoreo y revisión de las medidas de seguridad implementadas, amenazas y vulneraciones a las que están sujetos los datos personales contenidos en los sistemas y/o bases de datos personales, lo que permite definir nuevos controles por ejemplos la revisión y actualización de las contraseñas utilizadas para resguardar los datos personales en equipos cómputo, o bien realizar actualizaciones sustentadas de los mecanismos implementados, y por supuesto, monitorear las medidas de seguridad ya establecidas, recordemos que todo es susceptible de mejorar. Fundamentado por el Artículo 29 fracción VI de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas.

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

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

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

- Acciones desarrolladas para la ejecución de las medidas de control existentes
- Manifestación de seguridad y controles implementados en el tratamiento de datos personales que realice. De ser así, deberán incluir una explicación de tal actualización o modificación
- Indicar de manera clara la actualización de los aspectos siguientes:

- La incorporación de nuevos activos en el tratamiento que realiza, como podrían ser una actualización o modificación en el Hardware o software del sistema utilizado, personal de nuevo ingreso a cargo del tratamiento o cualquier otro recurso humano o material que tenga impacto en el tratamiento de los datos personales.
- El surgimiento de nuevas amenazas en el tratamiento de los datos.
- La posibilidad de que las nuevas amenazas que originen una vulnerabilidad en el tratamiento de datos
- La posibilidad de que las nuevas amenazas que originen una vulnerabilidad en el tratamiento de datos.

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

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

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

7. EL PROGRAMA GENERAL DE CAPACITACIÓN.

De conformidad con el artículo 29 fracción VII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, establece que en el documento de seguridad deberá integrarse el programa general de capacitación; el numeral 83, fracción XII de la propia Ley, indica que las Autoridades Garantes tendrán, entre otras atribuciones, facultades, competencias o funciones, promover la capacitación y actualización en materia de Protección de Datos Personales; de igual forma es importante destacar, que el dispositivo 35, fracción VI, de la Ley de Transparencia y Acceso a la Información Pública determina que es autoridad garante el órgano encargado de la Contraloría Interna, homologo o equivalente del Poder Legislativo. Ahora bien, de la lectura al numeral 40, fracción V, de la Ley de Transparencia Local se advierte que, el Comité de Transparencia promoverá y establecerá los programas de capacitación en materia de acceso a la información y accesibilidad para todas las personas servidoras públicas o integrantes del sujeto obligado; asimismo, el artículo 78, fracción VII, atribuye al Comité de Transparencia establecer los programas de capacitación y actualización para las personas servidoras públicas en materia de protección de Datos Personales.

De lo anterior, la capacitación y actualización se implementará conforme al Programa de Capacitación que establezca el Comité de Transparencia del H. Congreso del Estado. El órgano de la Contraloría Interna del H. Congreso del Estado conforme a sus atribuciones, facultades, competencias o funciones, colaborará para llevar a cabo las actividades de capacitación y actualización de las personas servidoras públicas del Poder Legislativo, privilegiando en todo momento las temáticas que favorezcan un amplio conocimiento de la materia de protección de datos personas.

ANEXO 1. BITACORA DE ACCESO Y VULNERACIONES DE SEGURIDAD DE LOS DATOS PERSONALES.

Las bitácoras de acceso y vulneraciones, serán emitidas por las áreas administrativas del Honorable Congreso del Estado de Chiapas que tratan datos personales, las bitácoras se emitirán de conformidad con el artículo 33 de la Ley de Protección de Datos en Posesión de Sujetos Obligados del Estado de Chiapas, en las que se describa lo siguiente:

- ✓ Fecha en la que ocurrió la vulneración
- ✓ Motivo de la vulneración
- ✓ Acciones correctivas implementadas de forma inmediata y definitiva.

H. CONGRESO DEL ESTADO DE CHIAPAS
JUNTA DE COORDINACIÓN POLÍTICA
UNIDAD DE TRANSPARENCIA

BITÁCORA DE VULNERACIONES

INFORMACIÓN DE QUIEN DETECTA EL INCIDENTE		
NOMBRE COMPLETO:		FIRMA:
PUESTO/CARGO:		
ÁREA DE ADSCRIPCIÓN:		
TELÉFONO:		

INFORMACIÓN SOBRE EL INCIDENTE		
FECHA Y HORA DEL INCIDENTE DE LA VULNERACIÓN:		
TIPO DE SOPORTE DE TRATAMIENTO:	FISÍCO ☐	ELECTRÓNICO ☐
NOMBRE DEL RESPONSABLE DEL PROCESO:		
LA INFORMACIÓN VULNERADA CONTIENE DATOS PERSONALES:	SI ☐	NO ☐
LA INFORMACIÓN VULNERADA ESTA REGISTRADA EN EL DOCUMENTO DE SEGURIDAD:	SI ☐	NO ☐
SELECCIONE EL TIPO DE VULNERACIÓN:	☐ Pérdida o destrucción no autorizada ☐ Robo, extravío o copia no autorizada ☐ Uso, acceso o tratamiento no autroizado ☐ Daño, alteración o modificación no autorizada ☐ Otro. Especifique:_____ ☐ Alerta de seguridad	

MOTIVO EN TORNO AL INCIDENTE OCURRIDO

FIRMA DE LOS RESPONSABLES	
_____	_____
NOMBRE Y FIRMA DEL RESPONSABLE DEL PROCESO	**NOMBRE Y FIRMA DEL TITULAR DEL ÁREA**

H. CONGRESO DEL ESTADO DE CHIAPAS
JUNTA DE COORDINACIÓN POLÍTICA
UNIDAD DE TRANSPARENCIA

BITÁCORA DE VULNERACIONES

ACCIONES CORRECTIVAS			
SISTEMA DE INFORMACIÓN O BASE DE DATOS VULNERADO:	FISÍCO: ☐	ELECTRÓNICO: ☐	MIXTO ☐
CANTIDAD DE TITULARES AFECTADOS:			
SOPORTE DE LA INFORMACIÓN VULNERADA:	FISÍCO: ☐	ELECTRÓNICO: ☐	MIXTO ☐
EL TRATAMIENTO FUE SUSPENDIDO/BLOQUEADO/RESGUARDADO	SI ☐	NO ☐	
ACCIÓN REALIZADA, (SINO SE REALIZÓ, EXPLICAR MOTIVO):			
HORA:	FECHA:		
TIPO DE DATOS PERSONALES COMPROMETIDOS:	☐ Identificativos ☐ Académicos ☐ Datos en procedimientos admvos. ☐ Sensibles	☐ Laborales ☐ Patrimoniales	

ACCIONES CORRELATIVAS IMPLEMENADAS	
ACCIONES CORRECTIVAS IMPLEMENTADAS DE MANERA INMEDIATA:	
ACCIONES CORRELATIVAS IMPLEMENTADAS DE FORMA DEFINITIVA:	

FIRMA DE LOS RESPONSABLES	
NOMBRE Y FIRMA DEL RESPONSABLE DEL PROCESO	NOMBRE Y FIRMA DEL TITULAR DEL ÁREA

ANEXO 2. CARTA DE CONFIDENCIALIDAD

La carta de confidencialidad forma parte integral del Documento de Seguridad del Honorable Congreso del estado de Chiapas, con la finalidad de establecer controles o mecanismos que tengan por objeto de que todas aquellas personas servidoras públicas del Poder Legislativo, que intervengan en cualquier fase del tratamiento de los Datos Personales guarden confidencialidad respecto de estos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo. Lo anterior, sin menoscabo de lo establecido en las disposiciones normativas de acceso a la información pública.

El propósito de la implementación de la carta de confidencialidad, es formalizar el compromiso ético y la obligación legal que asumen las personas servidoras públicas que, en el ejercicio de sus atribuciones, facultades, competencias o funciones, tengan acceso, manejen, traten o resguarden datos personales e información clasificada como reservada o confidencial, de igual manera se pretende dar estricto cumplimiento al deber de confidencialidad establecido en el artículo 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.

Mediante esta carta, que establece el deber ineludible de secrecía, uso exclusivo y custodia adecuada de la información institucional que contienen datos personales, se establecen medidas de seguridad de alto nivel, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los Datos Personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Lo anterior, sin afectar las acciones de vigilancia y verificación que realice la autoridad garante de la Contraloría Interna del Poder Legislativo.

CARTA COMPROMISO DE CONFIDENCIALIDAD

Lugar y Fecha: Tuxtla Gutiérrez, Chiapas; a _____de _____del 20__

I. DECLARACIÓN DE ADSCRIPCIÓN Y CARGO

El/La que suscribe, **[Nombre Completo del Servidor Público]** _____, en mi carácter de **[Puesto o Cargo]** _____, adscrito(a) a **[Área, Unidad Administrativa o Dirección]** _____, acepto las condiciones de resguardo, reserva, custodia, protección de la seguridad y confidencialidad de la información, datos personales y de todo tipo de documentos propiedad del H. Congreso del Estado (Poder Legislativo) o de la que tenga conocimiento, con motivo del trabajo, empleo, comisión ,integración del comité o cualquier órgano colegiado que sesione a fin de deliberar sobre procesos internos y/o dictaminar proyectos e iniciativas legislativas, así como para la toma de decisiones relativas a actividades administrativas dentro del poder legislativo.

II. MARCO NORMATIVO Y FUNDAMENTO LEGAL

El presente documento se sustenta rigurosamente en las disposiciones contenidas en:

- **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**. En los artículos 3 fracción XIV, 25, 36, 53 fracción V, 58 inciso d), 78, 115 y 132 fracción VII de la ley antes referida.
- **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas**, en los artículos 3 fracción XIII, 25, 36, 53 fracción V, 58 numeral I letra d), 61, 76 110 y 127 VIII de la ley antes referida.
- **Ley de Desarrollo constitucional, en los artículos 75, 76 y 77.**

III. CLÁUSULAS DE COMPROMISO

1. **Deber Estricto de Confidencialidad:** Me comprometo a guardar secreto absoluto y confidencialidad respecto a todos los datos personales y datos personales sensibles de los que tenga conocimiento o acceso directo o indirecto con motivo de las actividades administrativas, operativas o institucionales prestadas.
2. **Prohibición de Divulgación y Uso Indebido:** Queda estrictamente prohibido reproducir, transmitir, ceder, revelar, publicar o difundir por cualquier medio (físico, electrónico o digital) la información confidencial a personas no autorizadas, salvo autorización previa y expresa de los titulares o mandamiento escrito de autoridad competente.
3. **Finalidad Exclusiva:** La información personal será tratada única y exclusivamente para los fines inherentes a las atribuciones normativas que corresponden al cargo asignado y conforme a los Avisos de Privacidad institucionales aplicables.
4. **Cumplimiento de Medidas de Seguridad:** Acepto acatar puntualmente las medidas de seguridad físicas, técnicas y administrativas contempladas en el Documento de Seguridad de la institución para prevenir cualquier pérdida, alteración, destrucción o acceso no autorizado.

CARTA COMPROMISO DE CONFIDENCIALIDAD

5. **Subsistencia de la Obligación:** La obligación de guardar confidencialidad subsistirá de forma indefinida y permanente, **incluso después de haber concluido la relación laboral, contractual o administrativa** con el Honorable Congreso del Estado.

IV. Notificación de Incidentes y Sanciones Aplicables:
En caso de detectar alguna vulneración, brecha de seguridad o riesgo que comprometa la integridad de los datos personales, me obligo a informarlo inmediatamente a la Unidad de Transparencia del Honorable Congreso del Estado

El incumplimiento de los compromisos asumidos en este instrumento dará lugar al inicio de los procedimientos de responsabilidad administrativa conforme a la *Ley de Responsabilidades Administrativas para el Estado de Chiapas*.

FIRMANTE / SERVIDOR PUBLICO	**POR EL SUJETO OBLIGADO / TESTIGO**
[Nombre y Firma Autógrafa]	[Nombre del Titular de Recursos Humanos o Área]
	Sello o Validación de Recepción

CONCLUSION

El presente Documento de Seguridad del Honorable Congreso del Estado de Chiapas constituye el instrumento normativo y operativo clave para garantizar la protección, confidencialidad, integridad y disponibilidad de las bases de datos y la información sensible bajo el resguardo de esta Sede Legislativa.

A través de la implementación sistemática de medidas de seguridad de carácter administrativo, físico y técnicas, el Congreso del Estado ratifica su estricto apego a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, asegurando la mitigación de riesgos como el acceso no autorizado, la pérdida o el tratamiento indebido de los datos personales.

El Documento de Seguridad asegura el compromiso permanente de todas las personas servidoras públicas del Congreso del Estado, quienes asumen de forma individual e institucional el deber irrenunciable de guardar confidencialidad y aplicar las mejores prácticas institucionales, así como reportar oportunamente cualquier incidente que vulnere la seguridad de la información.