PODER LEGISLATIVO
DEL ESTADO LIBRE Y SOBERANO
DE QUINTANA ROO

DOCUMENTO DE SEGURIDAD DEL SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

INDICE

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

GLOSARIO

Bases de Datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento u organización.

Ciclo de vida: Tiempo que duración y conclusión del tratamiento de los datos personales, para después ser suprimidos, cancelados o destruidos por parte del responsable.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

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. Se consideran sensibles de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas, datos biométricos, preferencia sexual y de género.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

Finalidad: Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo, de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.

Instituto: Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo.

Ley de datos: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad a nivel organizacional, identificación, clasificación y borrado seguro de los datos personales, 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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades.

a) Prevenir el acceso no autorizado al perímetro de la organización del responsable sus instalaciones físicas, áreas críticas, recurso y datos personales.

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización del responsable, recursos y datos personales.
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización del responsable.
d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

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

a) Prevenir que el acceso a las bases de datos personales, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Responsable: Cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, que decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

Sistema de datos personales: Conjunto de organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los sujetos obligados, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Los sistemas de datos personales se distinguen en:

> **Físicos:** Conjunto ordenado de datos de carácter personal que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales.
>
> **Automatizados:** Conjunto ordenado de datos de carácter personal que permita acceder a la información relativa a una persona física utilizando una herramienta tecnológica.

Soporte electrónico: Son los medios de almacenamiento inteligibles solo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos, es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros), tarjetas de memoria (USB y SD) y demás medios de almacenamiento masivo no volátil.

Soporte físico: Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados "a mano" o "a máquina", fotografías, placas radiológicas, carpetas, expedientes, demás análogos.

Titular: La persona física a quien correspondan los datos personales.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados de manera enunciativa más no limitativa con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia y en general cualquier uso o disposición de datos personales.

Unidad de Transparencia: Instancia que auxilia, orienta, gestiona, establece, informa, propone, aplica, asesora, registra y realiza las gestiones necesarias para el manejo, mantenimiento, seguridad, y protección de los sistemas de datos personales en posesión del responsable.

Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

Vulneración de datos personales: Es la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

INTRODUCCIÓN

El presente documento de seguridad constituye el instrumento que describe y da cuenta sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el Poder Legislativo, para garantizar el cumplimiento de los principios y deberes establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Por lo anterior, se realizó e implementó un programa de capacitaciones especializadas en materia de protección de datos personales con la finalidad de concientizar a los servidores públicos sobre el trato lícito y adecuado de los datos personales.

El presente documento de seguridad es un conjunto de políticas, lineamientos y procedimientos establecidos por el Poder Legislativo con el fin de proteger la información y los datos personales. El objetivo principal es asegurar la confidencialidad, integridad y disponibilidad de la información, así como garantizar el cumplimiento de las normativas y regulaciones aplicables; con el siguiente conteniendo:

I) El inventario de datos personales y de los sistemas de tratamiento;
II) Las funciones y obligaciones de las personas que traten datos personales;
III) El análisis de riesgos y brecha;
IV) El plan de trabajo;
V) Mecanismos de monitoreo y revisión de medidas de seguridad y;
VI) El programa general de capacitación.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

Mismo que será de observancia obligatoria para todos los servidores públicos que intervienen en el tratamiento de datos personales que se encuentren en posesión de este Poder, que debido a la prestación de un servicio tenga acceso a los datos personales de conformidad con lo establecido en la LGPDPPSO.

Es menester señalar que este Poder Legislativo del Estado de Quintana Roo, a través de la Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en coadyuvancia con los enlaces de las áreas administrativas generadoras de la información, ha realizado acciones y actividades que tuvieron como finalidad de establecer los cimientos para la creación de este documento de seguridad; mismo que fue presentado y aprobado por el Comité de Transparencia, quien de conformidad con el artículo 83, segundo párrafo y 84, fracción I, de la Ley General, es la autoridad máxima en materia de protección de datos personales, contando con la atribución de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

OBJETIVO

Garantizar que todo tratamiento de datos personales cuente con las medidas de seguridad necesarias para la protección de los mismos y el cumplimiento de las obligaciones previstas en la Ley de datos.

De conformidad con el artículo 34 de la Ley de datos, establece que el responsable debe realizar las siguientes actividades interrelacionadas:

- Crear Políticas internas para la gestión y tratamiento de los datos personales.
- Las funciones y obligaciones del personal involucrado en el tratamiento de los datos personales.
- Realizar un inventario de datos personales y de los sistemas de tratamiento.
- Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes y los recursos involucrados.
- Monitorear y revisar de manera periódica las medias de seguridad implementadas.
- Realizar capacitaciones del personal.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

RESPONSABILIDADES

En apego al artículo 95 de la Ley de datos, establece que el Comité de Transparencia será la autoridad máxima en materia de protección de datos personales, dentro de sus funciones está la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales. En esa tesitura dicho órgano tiene las funciones siguientes:

I. Aprobar, supervisar y evaluar las políticas, programas, acciones, en conjunto con las áreas técnicas que estime necesario, involucrar o consultar;
II. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en el ámbito de organización del responsable, que resulten aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso;
III. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
IV. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;
V. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la Ley de datos y en aquellas disposiciones que resulten aplicables en la materia;
VI. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.
VII. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto Nacional.
VIII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

IX. Dar vista al órgano interno de control en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

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

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

MARCO NORMATIVO

- Constitución Política de los Estados Unidos Mexicanos. (CPEUM)
- Ley General de Transparencia y Acceso a la Información Pública. (LGTAIP)
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (LGPDPPSO)
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales).
- Ley Orgánica del Poder Legislativo del Estado de Quintana Roo.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

INVENTARIO DE DATOS PERSONALES

El Poder Legislativo se deposita para su ejercicio en una cámara de diputados denominada "Legislatura", integrada con diputados de mayoría relativa y de representación proporcional en los términos que previene la Constitución y esta ley, la cual se renovará en su totalidad cada tres años, funcionará en pleno y para el conocimiento, análisis y resolución de los asuntos de su competencia, se auxiliará de los siguientes órganos:

Órganos de Dirección:

a) Junta de Gobierno y Coordinación Política;
b) Mesa Directiva;
c) Comisión Permanente, y
d) Comisiones.

Órganos de Representación:

a) Grupos Legislativos;
b) Representaciones Legislativas;
c) Diputados Independientes, y
d) Diputados sin partido.

Órganos Técnicos y Administrativos:

a) Secretaría General;
b) Instituto de Investigaciones Legislativas;
c) Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, y
d) Las demás que coadyuven a las funciones de las anteriores.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

Con motivo de dichas funciones, la Institución es responsable del tratamiento de diversos datos personales, por lo que, con fundamento en lo dispuesto por los artículos 3 fracción XIV, 35, 83 y 84 fracciones I y II de la LGPDPPSO, así como en los artículos 55 a 64 de los Lineamientos Generales, este Sujeto Obligado, debe establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de estos.

El Poder Legislativo cuenta con 19 Unidades Administrativas que manifestaron dar tratamiento a datos personales, con las cuales se integró el inventario de datos personales, con el objeto de atender las disposiciones legales. Mismas que a continuación se relacionan:

1. Secretaria General.
2. Oficialía de Partes.
3. Unidad De Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
4. Órgano Interno de Control.
5. Coordinación de Comunicación Social.
6. Unidad de Igualdad de Género.
7. Unidad de Vigilancia de la Comisión de Hacienda, Presupuesto y Cuenta.
8. Dirección de Control del Proceso Legislativo.
9. Dirección de Análisis Jurídico Legislativo.
10. Dirección de Tecnologías de la Información.
11. Dirección de Archivo General y Biblioteca.
12. Dirección General Administrativa.
13. Dirección Jurídica.
14. Dirección de Finanzas.
15. Dirección de Modernización y Desarrollo Administrativo.
16. Dirección de Relaciones Públicas.
17. Dirección de Atención Ciudadana.
18. Dirección de Normatividad Contable.
19. Unidad de Desarrollo Humano y Bienestar Laboral.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

Para el debido cumplimiento de las obligaciones que se establecen en este documento, fue necesario que cada una de las unidades administrativas realizaran un diagnóstico de los tratamientos de datos personales que se llevan a cabo. Dicho diagnóstico se basa en la elaboración de un inventario de la información de cada tratamiento de los datos personales que se realizan en el Poder Legislativo.

Para ello, se identificaron las obligaciones que se deben cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas, de acuerdo con lo que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo y los Lineamientos Generales, y según el ciclo de vida de los datos personales.

Cabe destacar que este sujeto obligado procura la adopción de prácticas adecuadas para la protección de los datos personales en todos los tratamientos que así lo permitan.

Ahora bien, es preciso señalar que los medios para la obtención de los datos personales se llevan a cabo de la siguiente forma:

- Directamente del titular de forma escrita, expresa y tácita.

Entre estos se recaban datos identificativos, datos patrimoniales y datos sensibles. Para su uso se requiere el consentimiento del titular, el cual puede ser expreso o tácito dependiendo del dato personal a tratar, cuando se trata de datos sensibles, el consentimiento debe ser expreso y se debe solicitar de acuerdo con el tratamiento de datos personales al que pertenezca.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

Este inventario de datos personales permite el análisis, desarrollo y concreción de medidas para el adecuado tratamiento de datos personales al interior del Poder Legislativo, con el ánimo de sensibilizar a las y los servidores públicos en la importancia de garantizar las acciones mediante las cuales se posibilite el efectivo ejercicio de la autodeterminación informativa, acorde las medidas de seguridad recomendadas.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

Es de precisar que el Poder Legislativo, es el responsable sobre el tratamiento de los datos personales que se obtengan o utilicen con motivo de las facultades establecidas en su Ley Orgánica, y en ese sentido, todo el personal que por razón de sus funciones tenga acceso a los mismos debe atender al cumplimiento de los principios y deberes establecidos en la LGDPPSO, mismos que consisten en los siguientes principios:

- **Licitud**, implica que todo tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.
- **Lealtad**, implica 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.
- **Información**, implica que el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma: libre, especifica e informada.
- **Consentimiento**, mismo que podrá manifestarse de forma: expreso y tácito.
- **Finalidad**, implica que todo tratamiento de datos personales que efectué el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas.
- **Proporcionalidad**, implica que el responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad concreta, explícita lícita y legítima que justifica su tratamiento.
- **Calidad**, implica que, el responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se

altere la veracidad de éstos y según se requiera para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que motivaron su tratamiento.

- **Responsabilidad**, se traduce en que el responsable deberá implementar los mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en este ordenamiento; y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y al Instituto, debiendo observar para tal efecto la legislación aplicable en la materia. Así mismo, podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines, en lo que no se contraponga con la normativa mexicana.

Y en los siguientes deberes:

Seguridad, refiere a que los titulares de los datos personales tienen derecho a que la información personal que proporcionen a los responsables se resguarde bajo medidas de seguridad adecuadas, que eviten su pérdida, alteración, destrucción, daño o uso, acceso o tratamiento no autorizado. En ese sentido, los responsables estamos obligados a resguardar los datos personales en bases de datos protegidas con medidas de seguridad como son:

- **Medidas administrativas:** Implementar controles que ayuden a evitar prácticas inadecuadas del personal que pongan en riesgo los datos personales, por ejemplo, evitar compartir contraseñas o dejar los expedientes al alcance de personas que no estén encargadas de su estudio o tramitación.

- **Medidas físicas:** Controles aplicados en los espacios físicos e infraestructura que minimicen el robo o acceso no autorizado, por ejemplo, mantener las áreas de trabajo, mobiliario y equipos debidamente cerrados con los controles y candados suficientes.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

- **Medidas técnicas:** Controles para proteger equipos de cómputo y dispositivos de almacenamiento de virus, malware, entre otros.

Confidencialidad, de acuerdo con el artículo 42 de la LGDPPSO toda persona tiene derecho a que sus datos personales sean tratados con confidencialidad, es decir, a que éstos no se difundan o compartan con terceros, salvo que exista consentimiento para ello o alguna obligación normativa requiera su difusión. Ahora bien, sólo bajo ciertas circunstancias está permitida la comunicación de datos personales con terceros, principalmente si el titular de estos ha otorgado su consentimiento, pero también cuando se presente alguno de los siguientes supuestos:

- Cuando la transferencia esté prevista en una ley, convenios o Tratados Internacionales suscritos y ratificados por México;
- Cuando la transferencia se realice entre responsables del sector público, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- Cuando la transferencia sea necesaria para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;
- Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;
- Cuando la transferencia sea requerida para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

- Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero, o
- Cuando la transferencia sea necesaria por razones de seguridad nacional. En ese sentido, se solicita se considere lo anterior, y en el ámbito de su competencia, se dé cumplimiento a los principios y deberes que rigen la materia de protección de datos personales, a efecto de garantizar y proteger derechos de terceros.

Como se ha mencionado en líneas anteriores, de los objetivos que tiene este documento, es de fomentar en los sujetos obligados la importancia del adecuado tratamiento de los datos personales, de los cuales podemos mencionar los siguientes:

1. **Protección de la privacidad:** Los datos personales es información sensible y privada de los individuos, y su tratamiento inadecuado puede comprometer su privacidad. Al inculcar a los servidores públicos la importancia de tratar los datos personales de manera adecuada, se promueve el respeto a la privacidad de las personas y se evita cualquier uso indebido o acceso no autorizado a dicha información.
2. **Fomento de la confianza ciudadana:** Cuando los servidores públicos tratan los datos personales con responsabilidad y respeto, se fortalece la confianza de la ciudadanía en las instituciones y en el gobierno en general. Esto contribuye a una relación más sólida y positiva entre los ciudadanos y el sector público, lo que resulta fundamental para el adecuado funcionamiento de la administración y para promover la participación ciudadana.
3. **Preservación de la imagen institucional:** El tratamiento adecuado de los datos personales también tiene un impacto en la imagen y reputación de las instituciones públicas. El incumplimiento en la protección de la privacidad puede generar desconfianza y afectar negativamente la percepción que la ciudadanía tiene sobre la

institución. Por el contrario, al inculcar una cultura de protección de datos en los servidores públicos, se contribuye a preservar una imagen institucional sólida y confiable.

Es importante mencionar que este Sujeto Obligado, a través de la Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales ha generado los avisos de privacidad al inicio de los tratamientos de datos personales, con la finalidad de dar cumplimiento al Principio de información, establecido en los Artículos 27 y 28 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y del 26 al 45 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

El área denominada de Apoyo y Asistencia Legislativa del Poder Legislativo cuenta con **150 procedimientos**, específicamente de las Comisiones de los Diputados que integran esta XVII Legislatura, siendo las de: Gestión Social, Solicitudes, Comisiones, Iniciativas, Acuerdos e informes, en los que se recaban datos personales de identificación, de contactos, patrimoniales y sensibles.

Cabe mencionar, que la cantidad de datos personales que acopia el Poder Legislativo, en sus **240 procedimientos,** son principalmente datos personales de identificación, siendo la información concerniente a una persona física que permite diferenciarla de otras en una colectividad, tales como: nombre, Clave Única de Registro de Población (CURP), Registro Federal de Contribuyentes (RFC), año de nacimiento o edad, domicilio, firma, antecedentes laborales, cedula profesional, características físicas, correo electrónico, sexo, curriculum vitae, datos académicos, datos laborales, ocupación, nacionalidad, teléfono fijo o celular, datos sindicales, nivel educativo, títulos profesionales.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

Ahora bien, en 166 procedimientos, se utilizan datos personales patrimoniales, siendo esta información concerniente a una persona física relativa a sus bienes, derechos, cargas u obligaciones susceptibles de valoración económica, como son: datos contenidos en la declaración patrimonial, propiedades y bienes inmuebles, cuenta bancaria, saldos de cuentas bancarias, descuentos personales y beneficiarios.

En 168 procedimientos, se acopian datos de contacto, se refiere a información que permite mantener o entrar en contacto con su titular, tal como: domicilio; correo electrónico; teléfono fijo; teléfono celular, entre otros.

En 171 procedimientos, se acopian datos laborales, siendo esta información concerniente a una persona física relativa a su empleo, cargo o comisión; desempeño laboral y experiencia profesional, generada a partir de procesos de reclutamiento, selección, contratación, nombramiento, evaluación y capacitación, tales como: puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional; referencias laborales; fecha de ingreso y salida del empleo, entre otros.

En 182 procedimientos, se acopian datos sensibles, siendo estos los 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. Se consideran sensibles de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas, datos biométricos, preferencia sexual y de género.

La Unidad administrativa con mayor cantidad de procesos es la **Dirección General Administrativa** con 24 procedimientos, mientras que Oficialía de Partes, Dirección de Finanzas y la Dirección de Tecnologías de la Información, son las que menos desarrollan al llevar solo 1 proceso.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

En relación con esto se desglosa, lo siguiente: Todas las 19 unidades administrativas y las 25 comisiones, solicitan datos de identificación, 6 unidades administrativas y las 25 comisiones, recaban datos patrimoniales, 6 unidades administrativas y las 25 comisiones, recaban datos de contacto, 7 unidades administrativas y las 25 comisiones, recaban datos laborales y 8 unidades administrativas y las 25 comisiones, recaban datos sensibles.

Es importante recalcar que, los titulares de las áreas son los que deben generar acciones para contar con los avisos de privacidad necesarios para el tratamiento de datos personales, y es a través de la Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, quien orientara y auxiliara en el proceso de la elaboración de los avisos de privacidad cuando así se solicite.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

ANÁLISIS DE RIESGO

Uno de los puntos fundamentales para el funcionamiento de un órgano del Estado, es su capacidad para prever y evitar situaciones que podrían o no ocurrir, en especial cuando a diario las tecnologías de la información se encuentran en constante evolución. Por estos puntos, es importante contar con un análisis de Riesgo y Brecha en función a los riesgos a los cuales se puedan enfrentar los datos personales en su ciclo de vida. Es por ello por lo que en esta revisión se identifica el riesgo inherente asociado a la información personal durante su procesamiento por parte del Poder Legislativo al llevar a cabo sus funciones, con el objetivo de que la institución pueda prever dicho riesgo y resguardar la información.

De acuerdo con la LPDPPSOQROO, es responsabilidad de los sujetos obligados determinar el riesgo inherente de los datos personales que manejan al implementar medidas de seguridad. Para lograrlo, se debe llevar a cabo un análisis que tome en consideración las amenazas y vulnerabilidades que puedan afectar a los datos, así como los recursos utilizados en su tratamiento.

Con respecto a esto, en el documento "Manejo de Incidentes de Seguridad de Datos Personales" emitido por el INAI, se indican ciertos incidentes, los más comunes son:

- Robo de información en documentos y medios del almacenamiento desechados incorrectamente.
- Empleados que acceden a datos personales sin la autorización correspondiente.
- Empleados que revelan información a otras personas a través de engaños.
- Robo o pérdida de equipos de cómputo, laptops, teléfonos inteligentes, tabletas, o memorias extraíbles con información personal.
- Acceso ilegal a las bases de datos personales por un externo.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

Es por ello, que se tiene que elaborar un análisis de riesgo y brecha, respecto a la información recabada para poder detectar áreas de oportunidad y de mejora. Según lo estipulado por los Artículos 33 fracción IV y 35 fracción III de la Ley General de Datos, la evaluación de los riesgos de los datos personales es un requisito esencial que debe estar contemplado en el documento de seguridad. Este documento describe y detalla, en términos generales, las medidas de seguridad técnicas, físicas y administrativas adoptadas por el Poder Legislativo con el propósito de garantizar la confidencialidad, integridad y disponibilidad de este tipo de información que se encuentra bajo su custodia.

De acuerdo con la Ley General de Datos Personales en Posesión de Sujetos Obligados, en su capítulo II, el responsable de datos personales deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

En general se tiene que el Poder Legislativo cuenta con 19 unidades administrativas que recaban datos personales, a través de 90 procedimientos descritos con anterioridad.

En base a esto, se categorizaron los datos para poder analizar los riesgos de los datos personales que son objeto de tratamiento por:

- De identificación o contacto.
- Patrimoniales.
- Sensibles.

Por lo que se determinó que se trabajan con 3 categorías.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

De igual manera se valoró la probabilidad y el impacto de que en el proceso de su obtención, tratamiento, almacenamiento, transferencia, remisión, bloqueo, y/o eliminación se pueda causar un daño a titular.

Para el desarrollo del análisis, se recuperaron estas amenazas sustentadas en la Ley:

a. Robo, extravío o copia no autorizada.
b. Uso, acceso o tratamiento no autorizado.
c. Daño, alteración o modificación no autorizado.
d. Pérdida o destrucción no autorizada.

Cada dato personal tratado tiene asignado un valor de acuerdo con el riesgo que conlleva su tratamiento. La identificación y valoración del riesgo en cada proceso en que se tratan datos personales por las unidades administrativas del Poder Legislativo se basaron en una escala del 0 al 3 de la manera siguiente:

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
DATOS IDENTIFICATIVOS	BAJO	1
DATOS ELECTRÓNICOS, DOMICILIO, LABORALES, PATRIMONIALES, PROCEDIMIENTOS ADMINISTRATIVOS	MEDIO	2
DATOS SENSIBLES	ALTO	3

De igual manera, el riesgo inherente tiene otros factores, por ejemplo, el volumen de titulares que maneje la unidad o el tratamiento, de esta manera

puede incrementar el riesgo independientemente al dato que manejen, como se presenta a continuación:

NIVEL DE RIESGO POR TIPO DE DATO					
TIPO DE DATO/NÚMERO DE TITULARES	0 a 500	501 a 5,000	5,001 a 50,000	50,001 a 500,000	Más de 500,001
DATOS IDENTIFICATIVOS	1	1	1	1	1
DATOS ELECTRÓNICOS, DOMICILIO, LABORALES, PATRIMONIALES, PROCEDIMIENTOS ADMINISTRATIVOS	1	1	2	3	3
DATOS SENSIBLES	1	2	3	3	3

En cuanto al Poder Legislativo, del total de 90 tratamientos de datos personales, cuentan con el nivel descrito a continuación:

NIVEL DE RIESGO EN EL PODER LEGISLATIVO	
Riesgo	Número de Procedimientos
Bajo/1	71
Medio/1	157
Alto/1	12
Medio/2	0
Alto/2	0
Medio/3	0
Alto/3	0

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

Del análisis anterior, es importante ya que se puede visualizar, las consecuencias para los titulares que pudieran derivar de una vulneración de seguridad, entre las que se puede mencionar:

1. El tratamiento de los datos para finalidades distintas establecidas por el Aviso de Privacidad, incluso por un tercero: (Robo de Identidad, Fraude, Pérdida de privacidad, Discriminación y Acoso).
2. Daño reputacional. Las vulneraciones de seguridad pueden afectar la reputación del Poder Legislativo y de los involucrados. La pérdida de confianza del público puede tener consecuencias a corto y largo plazo en términos de la relación con la ciudadanía y con sus mismos empleados.
3. La destrucción no autorizada de la información o pérdida parcial que implique la afectación en la prestación de un servicio o trámite.
4. La alteración o modificación de los datos que pueda impedir temporal o definitivamente el cumplimiento de las finalidades para las cuales fueron recabadas.

Además de esto, los datos se ven expuestos a ciertas amenazas, como lo son:

a. Robo, extravío o copia no autorizada.
b. Uso, acceso o tratamiento no autorizado.
c. Daño, alteración o modificación no autorizado.
d. Pérdida o destrucción no autorizada.

El análisis de brecha es definido como un proceso que se usa para comparar el desempeño real de la institución, con el desempeño deseado, en este caso, comparar la situación deseada en cuanto a la seguridad de los datos personales tratados con la que en realidad se cuenta, para esto hay que analizar todas vertientes y situaciones de seguridad a las que nos podemos enfrentar, identificar quienes están involucrados, establecer las causas más relevantes que determinan la brecha, identificar las diferencias de comportamiento entre los sistemas o actores a comparar.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

En la realización del análisis de brecha, se debe considerar:

a) Medidas existentes y efectivas.
b) Medidas de seguridad faltantes.
c) Existencia de nuevas medidas de seguridad que puedan remplazar a las existentes.

El Poder Legislativo cuenta con ciertas medidas adoptadas por sus sujetos responsables en el trato de los datos personales, esto para garantizar la confidencialidad, integridad y disponibilidad de estos, las cuales se clasifican en físicas, administrativas y técnicas, mismas que se describen a continuación:

1. **Físicas**: Son el Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa mas no limitativa, se deben considerar las siguientes actividades:

    a. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
    b. Prevenir el daño o interferencia a las instalaciones físicas y áreas criticas de la organización, recursos e información;
    c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
    d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

2. **Administrativas:** Son las 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.

DOCUMENTO DE SEGURIDAD DEL SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

3. **Técnicas:** Son el 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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

    a. Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
    b. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
    c. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
    d. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

De acuerdo con los Lineamientos Generales Protección de Datos Personales, especifica que para la realización del análisis de brecha el responsable deberá considerar lo siguiente:

I. Las medidas de seguridad existentes y efectivas,
II. Las medidas de seguridad faltantes, y
III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

De las acciones que se están valorando a implementar, en relación con la existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente, se encuentran:

- Digitalización de archivos.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

- Instalación de centro de datos o de almacenamiento de datos alterno a la sede legislativa.

Las anteriores medidas de carácter físico y técnico tienen la finalidad de sistematizar la información, con el objeto de eficientar los procedimientos realizados por los sujetos responsables, promover la gestión documental y garantizar el ciclo de vida de los archivos, incrementar las medidas de control a documentación que contenga datos personales y, finalmente, prever cualquier afectación a los centros de datos que pudiera impedir su recuperación inmediata, parcial o total, al estar concentrados en la misma sede.

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, hemos logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

- Obtención de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del aviso de privacidad.
- No difundir el aviso de privacidad.
- Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, e incendios.
- Daño de la base de datos que contenga información confidencial.
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos.

DOCUMENTO DE SEGURIDAD DEL SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

- Falta de capacitación de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes.
- Alteración de la información. Ante dichos riesgos identificados es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.

ORIGEN DE LA AMENAZA	CAUSA	POSIBLES CONSECUENCIAS
Acceso de personas no autorizadas a los sistemas o plataformas oficiales.	Adquirir información o datos personales.	Acceso no autorizado. Divulgación de datos personales. Robo de información. Modificaciones no autorizadas. Robo de información.
Acceso de personas no autorizadas como criminales o traficantes de datos a los sistemas o plataformas oficiales.	Adquirir datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	Extorsiones. Ataques a personas. Robo de información. Vulneración a la seguridad física y mental de los ciudadanos. Robo de información.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales.	Obtener información para beneficio personal. Curiosidad. Error involuntario. Por fines económicos.	Ataque a otros servidores públicos. Robo de información. Pérdida de datos personales. Uso indebido de datos personales. Uso ilícito de datos personales. Robo de información. Extorsión.

DOCUMENTO DE SEGURIDAD DEL SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

		Modificaciones no autorizadas. Robo de información.
Daño físico.	Agua. Fuego. Accidentes. Corrosión.	Daño o pérdida de los datos personales.
Eventos naturales.	Desastres climatológicos. Fenómenos meteorológicos. Cualquier eventualidad por causa natural.	Daño o pérdida de los datos personales.
Fallas técnicas.	Pérdida de electricidad. Falla o pérdida de internet. Falla en sistemas, correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas.
Decadencias técnicas.	Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos de telecomunicaciones o cómputos. Cambios de voltaje.	Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas. Falta de mecanismos para identificar o autenticación de usuarios.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

	Falta de actualización de antivirus.	Robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Espacio donde se archiven.	Carencia de espacio. Espacio con poca seguridad. Espacio no adecuado. Falta de llaves o medidas de seguridad para accesos.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Daño y/o alteración de la base de datos que contenga información confidencial.	Carencia de un servidor o sistema que almacene los datos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la	Daño y/o pérdida de los datos personales. Modificaciones no autorizadas.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

	pérdida, robo o extravío de expedientes.	

Hasta el momento no se han identificado o reportado vulneraciones desde las áreas generadoras de información o las dependencias que integran el Poder Legislativo.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

ANÁLISIS DE BRECHA

Una vez identificados los posibles riesgos a los que este Poder Legislativo se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base las medidas de seguridad reportadas por las diversas unidades administrativas, las cuales consisten en lo siguiente:

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.
- El espacio físico o área donde se recaban datos personales es dentro de las instalaciones.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir si fue recabado frente a un escritorio, ventanilla, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos.
- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área.
- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.
- Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada está en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

Ahora bien, a efecto de evitar la vulneración de los datos personales en posesión de este Poder Legislativo, se considera que además de las medidas existentes, se puede reforzar la seguridad de la información con la adopción de las siguientes prácticas:

- **Control de acceso a la información**, consistente en mantener un control sobre las personas que recaban, administran, usan, almacenan o difunden datos personales. Dicho control puede realizarse a través de una bitácora en la que se señale el nombre y cargo del servidor público responsable, el proceso de tratamiento de datos personales que realiza, así como las medidas de seguridad que adopta a efecto de resguardar la información.
- **Activos del responsable**, la cual se refiere a la asignación de responsabilidades y a la clasificación de la información. En ese sentido, se propone que las áreas realicen un estudio pormenorizado acerca de los procesos que se vinculen con tratamiento de información confidencial, los tramos de responsabilidad de cada encargado de la información y se documenten mediante una bitácora.
- **Seguridad física**, en este apartado se sugiere tener más archiveros en buen estado y con seguridad para el resguardo de la información; en cuanto hace a la información que se resguarda de manera electrónica, se recomienda la actualización de los sistemas y el mantenimiento de los equipos.
- **Incidentes de seguridad de información**, en relación con este punto y derivado del diagnóstico realizado, no se ha presentado ninguna eventualidad en la cual se hayan vulnerados los datos personales, no obstante, se recomienda generar programas de capacitación respecto a las acciones a realizar ante una posible incidencia y de los mecanismos de mitigación del daño.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

CICLO DE VIDA

De conformidad con la fracción I del artículo 33 de la Ley General, para establecer y mantener las medidas de seguridad para la protección de los datos personales, se deberán crear políticas internas para su gestión y tratamiento que consideren el contexto en el que ocurren los tratamientos, así como el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior eliminación. Debido a ello, los Lineamientos Generales de Protección de Datos Personales, estipula que, en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, se deberá incluir la identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando su:

- Obtención de los datos personales
- Almacenamiento de los datos personales
- Uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
- Divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
- Bloqueo de los datos personales, en su caso, y
- Cancelación, supresión o destrucción de los datos personales

El Ciclo de vida de la información se refiere a los estados por los que pasa la información desde su creación/obtención hasta su destrucción/conservación. Al referirse al ciclo de vida de la información también se hace referencia al ciclo de vida de los datos personales, debido a que el dato personal forma parte de la información, que a su vez se encuentra contenida en diversos soportes documentales y formatos digitales.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

Vale la pena mencionar, de Acuerdo con Modelo de ciclo de vida de la información emitido por el INAI, este consta de cinco fases:

1. Creación/colecta/captura.
2. Procesamiento:

    a. Mantenimiento de datos/pre-procesamiento
    b. Almacenamiento
    c. Síntesis de datos/transformación
    d. Uso de la información

3. Transferencia/publicación/revelación
4. Archivado/retención
5. Destino final:

    a. Supresión/anonimización
    b. Conservación permanente

Con base en el Catálogo de Disposición Documental, se debe identificar si la información que contiene el dato personal se suprime, destruye o conserva como indefinida.

En caso de que sea necesario conservar la información solo para fines estadísticos, de investigación, entre otros, se debe aplicar un proceso de anonimización.
La anonimización es el proceso a través del cual se eliminan aquellos datos personales que permitan identificar directa o indirectamente a personas concretas, manteniendo solo información que no afecta a la privacidad y que puede ser usada para fines estadísticos, análisis, investigaciones, etc., esto es, variables genéricas como códigos postales, rangos de edad, medias de renta, nivel de estudios, etc.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

PLAN DE TRABAJO Y MEDIDAS DE SEGURIDAD

A continuación, conforme a los elementos identificados en el análisis de brecha se sugiere implementar las siguientes medidas de seguridad y plan de trabajo.

ACTIVIDADES	TEMPORALIDAD	ÁREAS INVOLUCRADAS	ACTUALIZACIÓN
Creación de políticas internas para el tratamiento de datos personales.	Anual	Delimitación del personal que maneja datos personales en todas las direcciones.	En acontecimientos que se susciten y los lineamientos que se publiquen.
Revisión de los inventarios de datos personales.	Anual.	Todas las direcciones.	Mensual.
Actualización, realización y monitoreo de la bitácora del manejo de datos personales.	Anual.	Comunicación directa con el responsable de la realización de esta, en cada dirección.	Mensual.
Establecer comunicación directa con la Unidad de Transparencia en relación con cuestionamientos relativos a la protección de datos personales.	Siempre que sea necesaria.	Director de área, enlace de transparencia o cualquier persona que maneje datos personales.	Siempre que sea necesaria.
Seguimiento al plan de capacitación en	Según la temporalidad	Personal que maneje datos personales.	Mensual.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

relación con la protección de datos personales.	de las sesiones establecidas.		
Revisión periódica de las medidas de seguridad señaladas en el documento de seguridad.	Mensual.	Personal que maneje datos personales.	Mensual.
Formular el análisis y matriz de riesgos.	Anual.	Personal que maneje datos personales.	Mensual.

Para garantizar la aplicación correcta de este sistema es necesario establecer los deberes de los servidores públicos que participan en el tratamiento de los datos personales derivado de sus atribuciones. Al momento de recibir los datos personales el servidor público que se encargue de su recepción deberá:

1. Tener a la vista el Aviso de Privacidad.
2. Dar a conocer el aviso de privacidad al titular de los datos personales previo a la obtención de sus datos.
3. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.
4. Al obtener los datos personales cerciorarse de que la información esté completa, actualizada, sea veraz, y comprensible.
5. Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales, ello cuando se dé cuenta.
6. Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.
7. Recabar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

8. Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.
9. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
10. Tomar, los cursos programados, respecto al taller o capacitación sobre el tratamiento de datos personales.

El servidor público involucrado en el tratamiento de datos personales deberá:

1. Conocer, aplicar y sujetarse al Aviso de Privacidad.
2. Aplicar las medidas de seguridad correspondientes a los datos personales tratados y/o el sistema de protección en el que participa.
3. Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.
11. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.
4. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
5. Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.
6. Tomar, una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.

El servidor público que administra los datos personales, conforme los sistemas de tratamiento vigentes deberán:

1. Conocer, aplicar y sujetarse al Aviso de Privacidad.
2. Conocer e implementar las medidas de seguridad establecidas en el documento de seguridad.
3. Aplicar nuevas medidas de seguridad que resulten accesibles y viables para la protección de datos personales.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

4. Supervisar a los servidores públicos que participan en la recepción y en el tratamiento de datos personales en cada trámite o sistema.
5. Tratar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.
6. Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.
7. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
8. Tomar, una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.
9. Informar a los titulares de los datos sobre nuevas finalidades del tratamiento de datos personales o nuevas transferencias.
12. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.
10. Informar a la Unidad de Transparencia sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.
11. Acudir a la Unidad de Transparencia en caso de asesoría sobre el tratamiento de datos personales.
12. Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.
13. Dar aviso al Comité de Transparencia, a través de la Unidad de Transparencia, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de estas.

El servidor público responsable de cada sistema, o en su caso, el titular de la Unidad Administrativa responsable de cada sistema deberá:

1. Conocer, aplicar y sujetarse al Aviso de Privacidad.

**DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO**

2. Implementar las medidas de seguridad que establece el documento de seguridad.
3. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
4. Tomar los cursos, taller o capacitación sobre el tratamiento de datos personales.
5. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.
6. Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.
7. Informar a la Unidad de Transparencia sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.
8. Monitorear la implementación de las medidas de seguridad.
9. Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de estas.
10. Dar aviso al Comité de Transparencia, a través de la Unidad de Transparencia, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de estas.
11. Presentar propuestas de mejora o modificación del documento de seguridad a través de la Unidad de Transparencia.
12. Emitir reportes en relación con el tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través de la Unidad de Transparencia.
13. Diseñar, desarrollar e implementar políticas públicas, procesos internos, y/o sistemas o plataformas tecnológicas necesarias para el ejercicio de sus funciones apegándose en todo momento al documento de seguridad, las políticas o lineamientos que para el tratamiento de datos personales que emita el Comité de Transparencia.
14. Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.

DOCUMENTO DE SEGURIDAD DEL
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES DEL
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO

PROGRAMA GENERAL DE CAPACITACIÓN

De acuerdo con lo establecido en el artículo 35 fracción VII de la LGPDPPSO, esta Institución debe realizar un programa de capacitación, y en ese sentido, se plantea generar un programa anual para desarrollar la cultura en seguridad de la información, conforme a los siguientes ejes:

a. Programas a corto plazo para la difusión en general de la protección de datos personales en la organización y su importancia en el entorno laboral.
b. Programas a mediano plazo que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales y;
c. Programa general a largo plazo que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de organización de la Institución.

Finalmente, conforme a lo establecido en la LGPDPPSO y en los Lineamientos Generales, el presente documento deberá actualizarse por lo menos una vez al año, en función de las medidas de seguridad adoptadas o de las nuevas circunstancias que se presenten en materia de seguridad y protección de datos personales.