



## UNIDAD DE TRANSPARENCIA

DEPENDENCIA:	CONGRESO DEL ESTADO.
ADSCRIPCIÓN:	UNIDAD DE TRANSPARENCIA.
OFICIO:	UT/615/2024
ASUNTO:	SE NOTIFICA RESPUESTA A SU SOLICITUD DE INFORMACIÓN.

*"2024, Año de los Pueblos Yumanos, Pueblos Originarios y de las Personas Afromexicanas"*

### C. SOLICITANTE P R E S E N T E.-

Anteponiendo un cordial saludo, me dirijo a usted a fin de notificar la presente determinación en atención a su solicitud identificada con el número de folio **24000198** y que de manera textual indica lo siguiente:

*"Folio: 020058024000198*

*Fecha de presentación: 02/08/2024*

*Nombre del solicitante:*

*Sujeto Obligado Congreso del Estado de Baja California*

*Tipo de solicitud: Información pública*

*Modalidad de entrega de la información:*

*Electrónico a través del Sistema de Solicitudes de Acceso a la Información de la PNT*

*Descripción de la solicitud:*

*Por medio de la presente se solicita versión digital (y en versión pública de ser el caso) de su Política de Gestión para el Tratamiento de Datos Personales (u homónimas), documento que se contempla en el artículo 33 fracción I de la Ley General de Protección de Datos Personales en Posesión de sujetos Obligados.*

*En caso de no contar con una política para la gestión y tratamiento de los datos personales, fundamentar la falta de esta.." (SIC)*

Por medio del presente y con fundamento en lo dispuesto por **de la Ley Orgánica del Poder Legislativo del Estado de Baja California**; le remito en documento anexo las *"POLÍTICAS INTERNAS DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DEL CONGRESO DEL ESTADO DE BAJA CALIFORNIA"*

En atención a lo anterior remito a usted, respuesta a su solicitud de información, en observancia a lo estipulado en el artículo 6 de la Constitución Política de los Estados



## UNIDAD DE TRANSPARENCIA

---

Unidos Mexicanos; Apartado C del Artículo 7 de la Constitución Política del Estado Libre y Soberano de Baja California, así como en los artículos 55, 56 fracción II, 113, 114, 115, 116, 117 y 118 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California.

Quedo a sus órdenes para cualquier duda o aclaración en el correo electrónico [unidad.transparenciabc@gmail.com](mailto:unidad.transparenciabc@gmail.com)

**ATENTAMENTE**

**MEXICALI, BAJA CALIFORNIA, A 29 DE AGOSTO DE 2024**

  
**LIC. DAVID GERSON CORPUS CAMPOS**  
**ENCARGADO DE DESPACHO DE LA UNIDAD DE TRANSPARENCIA**  
**DE LA H. XXV LEGISLATURA DEL CONGRESO DEL ESTADO DE BAJA CALIFORNIA.**





## **POLÍTICAS INTERNAS DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DEL CONGRESO DEL ESTADO DE BAJA CALIFORNIA**

### **OBJETIVO**

Instrumentar las directrices normativas que rijan las actividades internas del Congreso del Estado para cumplir con los principios, deberes y obligaciones previstos por la Ley General, así como la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado, en el tratamiento de datos personales a fin de garantizar el derecho humano a la protección de datos personales que establece el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

### **ÁMBITO DE APLICACIÓN**

Son de observancia general y aplicación obligatoria para todas las áreas administrativas, así como para las personas servidoras públicas del Congreso del Estado que conforme a sus atribuciones realicen tratamiento de datos personales.

### **PRINCIPIOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES**

El artículo 8 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Baja California, establece que en todo tratamiento de datos personales se deberá observar los principios rectores de la protección de datos personales:

- a. Licitud.
- b. Finalidad.
- c. Lealtad.
- d. Consentimiento.
- e. Calidad.
- f. Proporcionalidad.
- g. Información.
- h. Responsabilidad.

En observancia al correcto tratamiento de los datos personales en posesión de este Sujeto Obligado, la aplicación de los Principios Generales de Protección de Datos Personales, se formalizan como sigue:



**Principio de Licitud.**

Llevar a cabo el tratamiento de los datos personales de conformidad con las atribuciones o facultades que establecen las leyes en materia de protección de datos personales.

**Principio de Finalidad.**

1. Verificar que los tratamientos de datos personales que se realicen atiendan los fines específicos o determinados (finalidades concretas, lícitas, explícitas y legítimas) y que sean acordes a las atribuciones o facultades de este Sujeto Obligado.
2. Verificar que las finalidades para el tratamiento de los datos personales estén relacionadas con las atribuciones normativas de este Congreso del Estado.
3. Identificar las finalidades que no fueron informadas en los avisos de privacidad, verificando que estas se encuentren dentro de las atribuciones legales para el tratamiento de los datos personales y recabar el consentimiento del titular al momento de obtener sus datos personales.

**Principio de Lealtad.**

1. Garantizar que los datos personales recabados por este sujeto obligado, no se obtengan a través de medios engañosos o fraudulentos.
2. Garantizar y supervisar que los tratamientos de datos personales que lleva a cabo este Sujeto Obligado, no den lugar a la discriminación, trato injusto o arbitrario en contra del titular.

**Principio de Consentimiento.**

1. Garantizar que previo a la obtención de los datos personales de los titulares y después de haberles puesto a disposición los avisos de privacidad, se cuente con su consentimiento (tácito o expreso), verificando que el consentimiento que se obtenga de los titulares sea libre, específico e informado.
2. El consentimiento tácito se obtiene después de haber puesto a disposición del titular, el aviso de privacidad, y éste no manifiesta oposición u objeción alguna; asimismo, el consentimiento es tácito, cuando el tratamiento de datos actualiza alguno de los supuestos establecidos en el artículo 11 de la ley de la materia.
3. Se deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, cuando se trate de datos personales sensibles.

**Principio de Calidad.**

1. Adoptar las medidas necesarias, para mantener exactos, completos, correctos y actualizados los datos personales que son tratados por este Sujeto Obligado.



2. Establecer los plazos de conservación de los datos personales, los cuales no deben exceder del tiempo estrictamente necesario para llevar a cabo las finalidades que justifican el tratamiento ni aquel que se requiera para cumplir con las disposiciones normativas de que se trate (administrativo, jurídico, contable, fiscal, histórico, etc.)

**Principio de Proporcionalidad.**

1. Garantizar que los datos personales que se recaben sean los adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento, de igual manera que contengan los datos mínimos necesarios en relación a las finalidades que justifican su tratamiento.

**Principio de Información.**

1. Poner a disposición del titular los avisos de privacidad que correspondan antes y después de la obtención de los datos personales.

2. Implementar mecanismos para que el titular pueda manifestar su negativa para el tratamiento de datos personales para finalidades o transferencias que requieran su consentimiento.

3. Difundir los avisos de privacidad por medios electrónicos y físicos.

4. Ubicar los avisos de privacidad en lugares visibles que faciliten la consulta del titular.

5. Verificar que los avisos de privacidad integrales se encuentren de manera permanente en el portal de internet de este Congreso del Estado

**Principio de Responsabilidad.**

1. Elaborar políticas y programas de protección de datos personales, tomando en cuenta el desarrollo tecnológico y las técnicas existentes.

2. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y deberes en materia de protección de datos personales.

3. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

4. Establecer un sistema de supervisión y vigilancia interna y/o externa, para comprobar el cumplimiento de las políticas de protección de datos personales.

5. Garantizar que las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la ley general de protección de datos personales en posesión de sujetos obligados.





## **DE LAS OBLIGACIONES**

Todas las personas servidores públicos que intervengan en cualquier tipo de tratamiento de datos personales, así como las áreas responsables deberán realizar lo siguiente:

1. Atender las solicitudes de derechos ARCO conforme procedimiento Interno difundido por la Unidad de Transparencia.
2. Revisar que las actividades de tratamiento de datos personales que se realicen cuenten con sus avisos de privacidad y estos se difundan en los medios desde los cuales se recaban los datos sujetos a tratamiento.
3. Dar vista al Comité de Transparencia, a través de la Unidad de Transparencia, de cualquier vulneración o tratamiento indebido de datos personales de los que se tenga conocimiento.
4. Asegurar que el acceso a datos personales en posesión del área administrativa correspondiente sea únicamente por el personal autorizado.
5. Solicitar el asesoramiento del personal de la Unidad de Transparencia cuando estimen necesaria su intervención con el objeto dar cumplimiento a los principios, deberes y obligaciones en materia de protección de datos personales.

### **Del deber de confidencialidad**

Las personas y servidores públicos que traten datos personales, así como, en su caso, los despachos de asesores externos, deben guardar absoluta discreción sobre la información y los datos personales que generen, posean o deban conocer por razón de su encargo; la obligación de confidencialidad debe subsistir aun después de finalizada la relación entre el servidor público o el despacho, con el responsable.

### **Del deber de seguridad**

Las medidas de seguridad implementadas están orientadas a garantizar la confidencialidad, integridad y disponibilidad de los datos personales y la información que obra en los registros y bases de datos.

### **Medidas de seguridad administrativas:**

-Declaración de confidencialidad de los servidores públicos y encargados que tratan datos personales;



- Identificación de roles y perfiles de los servidores públicos y encargados que intervienen en los tratamientos de datos personales;
- Procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional;
- Programa de sensibilización, formación y capacitación en la materia a todo su personal;
- Esquema de derechos y contraseñas de acceso a las bases de datos y áreas críticas donde se encuentran la información;
- Avisos de privacidad;
- Bitácora para registrar y reportar las vulneraciones ocurridas a las bases y datos personales, debe incluir: fecha y lugar en donde se produjo, nombre y cargo del servidor público que notifica la incidencia, nombre y cargo del servidor público encargado de implementar las medidas de seguridad para mitigar la vulneración y, descripción de las acciones llevadas a cabo y las medidas de seguridad implementadas;
- Mecanismos para la identificación, clasificación y borrado seguro de los datos personales;
- Programa de depuración de archivo (de las bases de datos físicas y electrónicas) conforme a los plazos de conservación y parámetros dispuestos la normativa archivística, documentando los periodos de conservación de las bases de datos, del bloqueo (cuando sea necesario) y de supresión de las mismas;
- Bitácora de registro de personal que tiene acceso al archivo físico y a los expedientes, que incluya la finalidad para la cual se consulta tal expediente.

**Medidas de seguridad físicas:**

- Señalamientos de restricción en las áreas críticas donde se resguardan datos personales;
- Restricción de acceso a las áreas críticas solo al personal autorizado;
- Uso de candados en áreas clave.
- Registro de visitas o ingreso de personas ajenas al Congreso del Estado;
- Política de “escritorio” limpio al ausentarse temporalmente o bien, al finalizar el turno laboral.



- Dejar el área de trabajo en un estado que no permita a otros usuarios y/o personas no autorizadas, visualizar los datos e información a su cargo;
- No dejar a la vista documentos que contengan información confidencial;
- Bloquear el equipo de cómputo con contraseña, o bien, desconectarse y apagar el equipo.
- Recoger originales de impresoras y fotocopadoras, revisar la bandeja de entrada y de salida y retirar todos los documentos.
- Supresión de documentos utilizando trituradora, o bien, algún otro mecanismo que no permita su recuperación;
- No introducir softwares que no hayan sido validados y autorizados por el personal del área informática.

**Medidas de seguridad técnicas:**

- Uso de contraseñas personales e intransferibles.
- Realizar copias de seguridad, respaldos;
- Notificar cualquier falla del equipo de cómputo al área especializada para atenderla;
- Instalar antivirus y dar mantenimiento preventivo a los equipos de cómputo;
- Prohibir del uso de puertos USB por personas ajenas a la organización;
- Crear perfiles de acceso, claves y contraseñas de autenticación del personal que trata datos personales.

**De la relación con despachos de asesores externos.**

En caso de establecerse contratos de colaboración con despachos de asesoría externa, éstos deben adherirse al cumplimiento de los principios y deberes en materia de protección de datos personales, a través de la suscripción de cláusulas que lo describan claramente.