POLÍTICA DE GESTIÓN DE DATOS PERSONALES DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS DEL ESTADO DE COLIMA

Contenido

1. Objetivo.

Definir y establecer los principios generales o criterios de acción que servirán de guía en el proceso de toma de decisiones y en la actuación de los servidores públicos en los diferentes procesos que implica el tratamiento de los datos personales, al ejecutar los objetivos institucionales al interior del Instituto de Transparencia, Información Pública y Protección de Datos del Estado de Colima (INFOCOL), en la materia.

2. Fundamento legal.

El INFOCOL, de conformidad con el artículo 37 de los Mecanismos para el cumplimiento del principio de responsabilidad, enmarcado en la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima, tiene el deber definir y establecer políticas de seguridad en caminadas a la al tratamiento integral y protección de los datos personales, mediante una serie de acciones interrelacionadas, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

3. Ámbito de aplicación

Las políticas contenidas en el presente documento son de aplicación general para todos aquellos servidores públicos del Instituto de Transparencia, Información Pública y Protección de Datos del Estado de Colima (INFOCOL), que en el ejercicio de sus funciones realicen cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales la 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, de conformidad con el artículo 4 fracción XXXII de la ley antes referida.

4. Cumplimiento de los Principios y Deberes en materia de Protección de Datos Personales.

Principios.

Haciendo un ejercicio arbitrario de interpretación, la parte moral y ética de la propia Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima, es precisamente dar cumplimiento a todos los principios que establece el artículo 15 de la Ley:

I. Licitud;
II. Finalidad;
III. Lealtad;
IV. Consentimiento;
V. Calidad;
VI. Proporcionalidad;
VII. Información; y
VIII. Responsabilidad en el tratamiento de los datos personales.

I) Tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable (principio de licitud);
II) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad (principio de finalidad);
III) No obtener los datos personales a través de medios fraudulentos (principio de lealtad);
IV) Sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley (principio de consentimiento);
V) Procurar que los datos personales tratados sean correctos y actualizados; suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron; tratar datos personales estrictamente el tiempo necesario

para propósitos legales, regulatorios o legítimos organizacionales (principio de calidad);

VI) Tratar los menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en el aviso de privacidad (principio de proporcionalidad);

VII) Informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad (principio de información);

VIII) Velar por el cumplimiento de estos principios y adoptar las medidas necesarias para su aplicación (principio de responsabilidad);

Deberes.

Por otra parte, se encuentran los Deberes en materia de Protección de Datos Personales, estipulados en los artículos del 38 al 49 de nuestra ley en la materia. El Deber de Seguridad y de Confidencialidad en este sentido, nos obliga a tener herramientas normativas bien definidas para la prevención y actuación en caso de vulneraciones y fallas en las medidas de seguridad para la protección de los datos, entre otras cosas:

a) Establecer y mantener medidas de seguridad (deber de seguridad);

b) Guardar la confidencialidad de los datos personales (deber de confidencialidad);

c) Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos de la organización se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen;

d) Mantener un inventario actualizado de los datos personales o de sus categorías que maneja la organización;

e) Respetar los derechos de los titulares en relación con sus datos personales;

f) Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales;

g) Desarrollar e implementar un Sistema de gestión para las Medidas de Seguridad de los Datos Personales (SGSDP) de acuerdo a la política de gestión de datos personales, y

h) Definir las partes interesadas y miembros de la organización con responsabilidades específicas y a cargo de la rendición de cuentas para el (SGSDP).

5. Controles para garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personales.

La Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima, establece en su artículo 40, que los responsables deben garantizar la confidencialidad, integridad y disponibilidad de los datos personales en su posesión; lo anterior, a través de la medidas de seguridad, más específicamente de las medidas de seguridad Técnicas, Físicas y Administrativas.

5.1 Controles de Confidencialidad.

- Como medida de control primordial, todo el personal del INFOCOL deberá guardar confidencialidad permanente de los datos personales a los que tenga acceso.
- Para formalizar el mecanismo anterior, todo el personal deberá firmar carta compromiso de confidencialidad en este sentido.
- Se podrán desclasificar datos personales solo en los casos que la Leyes en la materia señalen.
- La Secretaría de Protección de Datos Personales del INFOCOL impartirá capacitaciones periódicas para todo su personal, en materia de medidas de seguridad para la protección de datos personales.
- El personal está obligado a cumplir con las medidas de seguridad físicas, técnicas y administrativas señaladas en el Documento de Seguridad.
- Se realizará una revisión periódica de las medidas de seguridad; físicas, técnicas y administrativas del instituto.

5.2. Controles de Integridad.

- Los datos personales deberán conservarse en el estado en que son recabados, asimismo los documentos que resulten del aprovechamiento de los datos personales deberán ser conservar su integridad.
- El personal conservará los datos personales que se encuentren en formato físico conforme a lo señalado por las medidas de seguridad físicas contenidas en el Documento de Seguridad.
- El personal conservará los datos personales que se encuentren en formato electrónico conforme a lo señalado por las medidas de seguridad técnicas contenidas en el Documento de Seguridad.
- El personal deberá mantener un formato de inventario de datos personales permanente y actualizado, de tal manera que se describa e identifique plenamente los tipos de dato que gestiona y debe proteger.

5.3. Controles de Disponibilidad.

- Se realizará una digitalización completa de la información que ingresa a través de la oficialía de partes y se almacena en discos duros.
- Una operación de respaldo incremental solo copia los datos que han variado desde la última operación de respaldo de cualquier tipo. Se utiliza la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último respaldo.
- Deberá realizarse un respaldo incremental de la información de cada área 1 vez al mes y almacenarlo en discos duros.
- Cada área será la responsable de almacenar sus respaldos durante el tiempo que señale el catálogo de disposición documental del Instituto, atendiendo, a las recomendaciones de la Secretaría de Archivos, así como de la Secretaría de Protección de Datos Personales del INFOCOL.

6. Acciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico.

Un incidente de seguridad es un riesgo materializado, en este sentido, la gestión de incidentes es el proceso de planeación, comunicación y capacidad de acción cuando ocurre un incidente de este tipo. Resulta entonces de primordial importancia contar con un plan de respuesta a los mismos, estableciendo claramente la relación entre (i) las alertas y los incidentes de seguridad, (ii) las características particulares de un incidente de seguridad cuando involucra datos personales y; (iii) las etapas del plan de respuesta a incidentes de seguridad, el cual se encuentra contenido en el Documento de Seguridad para la Protección de los Datos Personales del INFOCOL. En relación a los respaldos incrementales contienen fecha y hora, tanto inicial como final. La recuperación se realizará cruzando la fecha del incidente y el último respaldo.

Dentro de las acciones principales a ejercer, se encuentra la de informar de lo ocurrido al titular de los datos personales vulnerados, como lo estipula el artículo 40 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, y el artículo 49 de nuestra ley local en la materia. Por tanto, tener en cuenta que en el sector público, estos incidentes consideran:

a) Informar a los titulares de los datos personales lo siguiente:

1. La naturaleza del incidente.
2. Los datos personales afectados.
3. Las recomendaciones al titular acerca de las medidas que éste puede adoptar para protegerse.
4. Las acciones correctivas realizadas de forma inmediata.

5. Los medios donde los titulares pueden obtener más información.
6. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente.
7. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

b) Informar al Órgano Garante local (INFOCOL) de la vulneración de seguridad ocurrida.

c) La actualización del documento de seguridad correspondiente.

d) Contar con una bitácora de las vulneraciones en la que se describa:
1. En qué consistió la vulneración.
2. La fecha en la que ocurrió.
3. El motivo o causa de la vulneración.
4. Las acciones correctivas implementadas de forma inmediata y a largo plazo.

e) La imposición de sanciones por la autoridad correspondiente debido a la falta de implementación de medidas de seguridad.
Aunado a lo anterior, existen las denominadas revelaciones, las cuales son incidentes de seguridad que exponen la información a través de Internet o en medios masivos de comunicación. Las revelaciones de información pueden resultar en una vulneración de seguridad graves al exponer datos personales a un sin número de terceros. Cuando se identifica que una revelación expone datos personales, el responsable debe tomar todas las medidas que estén a su alcance para mitigar la difusión o publicación de los mismos. Por ejemplo, solicitar la baja de contenido al administrador de una página web, así como pedir la eliminación de resultados de un motor de búsqueda, a fin de minimizar el daño a los titulares.

7. Medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales.

En caso de detectarse una posible vulneración de datos personal deberá realizarse lo siguiente:

a) Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.

b) En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes.

c) Llenado de Formato B, señalado en el Documento de Seguridad del Instituto, por parte de la persona que detectó la vulneración.

d) Llenado de Formato B (Hoja 2), señalado en el Documento de Seguridad del Instituto, por parte de personal de la Secretaría de Protección de Datos Personales del INFOCOL.

e) Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.

f) Elaboración de Informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia.

g) Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales.

h) Llenado de la bitácora de vulneraciones conforme al artículo 48 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima.

8. Proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia.

La Secretaría de Protección de Datos Personales del INFOCOL, elaborará un plan anual de evaluación las políticas, procedimientos y planes de seguridad que será presentado, y en su caso, aprobado por Comité de Transparencia del Instituto.

9. Controles para garantizar que únicamente el personal autorizado podrá tener acceso a los datos personales para las finalidades concretas, lícitas, explícitas y legítimas que originaron su tratamiento.

Los empleados del Instituto deben portar su identificación institucional que cuenta con la siguiente información:

Al frente:

- ✓ Nombre.
- ✓ Cargo.

Al reverso:

- ✓ Vigencia.
- ✓ Número de empleado.
- ✓ Firma del titular de la institución.
- ✓ Sitio oficial.
- ✓ RFC.
- ✓ Domicilio de la institución.
- ✓ Teléfono de la institución.

10. Medidas preventivas para proteger los datos personales contra vulneraciones y tratamiento no autorizado.

- La Secretaría de Protección de Datos Personales, llevará a cabo capacitaciones periódicas con el objeto de prevenir acciones que contravengan las disposiciones normativas Generales y locales en materia de protección de datos personales.
- El personal de la Secretaría de Protección de Datos Personales llevará acabo auditorias periódicas, semestrales a las áreas que recaban y gestionan datos personales para verificar el cumplimiento de lo establecido en las herramientas normativas de protección de datos, como lo es el documento de seguridad del INFOCOL.