DOCUMENTO DE SEGURIDAD

COTAIPEC

COMISIÓN DE TRANSPARENCIA

Y ACCESO A LA INFORMACIÓN PÚBLICA

DEL ESTADO DE CAMPECHE

C O N T E N I D O

		Página
I.	Introducción……..	2
II.	Glosario…….	3
III.	Nombre de los sistemas de tratamiento o base de datos personales y nombre, cargo y adscripción del administrador…….	5
IV.	Funciones y obligaciones del responsable…….	7
V.	Inventario de los datos personales tratados……...	9
VI.	Estructura y descripción de los sistemas de tratamiento y/o base de datos personales…….	14
VII.	Controles y mecanismos de seguridad para las transferencias……..	19
VIII.	Resguardo de soportes físicos y/o electrónicos……	21
IX.	Bitácoras de acceso operación cotidiana y vulneraciones a la seguridad de los datos personales..	29
X.	Análisis de riesgos……..	31
XI.	Análisis de brecha……...	36
XII.	Gestión de vulneraciones……..	38
XIII.	Medidas de seguridad……	39
XIV.	Controles de identificación y autenticación de usuarios……...	47
XV.	Procedimiento de respaldo y recuperación de datos personales……	48
XVI.	Plan de contingencia……..	49
XVII.	Técnicas de supresión y borrado seguro de los datos personales…….	54
XVIII.	Plan de trabajo…….	55
XIX.	Mecanismos de monitoreo y revisión de las medidas de seguridad……..	56
XX.	Programa general de capacitación……..	57
XXI.	Anexos……..	58

I. INTRODUCCIÓN

La Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, en su calidad de responsable, a fin de dar cumplimiento al deber de Seguridad y en completo apego a las disposiciones contenidas en el *Capítulo III De los deberes y las medidas de seguridad de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Campeche*, ha establecido un conjunto de procesos y sistemas diseñados para la protección de los datos personales a los cuales tenga acceso a su tratamiento de acuerdo a sus funciones y atribuciones de ley.

En tal sentido, dentro de las acciones a emprender en toda institución para cumplir con dicho deber, se encuentra la actualización del documento de seguridad, instrumento que dará cuenta de todas las medidas, acciones, actividades, controles o mecanismos, implementados por el responsable con el objeto de garantizar que el tratamiento de los datos personales que realiza sea conforme a las disposiciones contenidas en la normatividad de la materia.

Por lo anterior, la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, procede a integrar y someter ante el Comité de Transparencia para su aprobación el presente documento de seguridad en cumplimiento a lo dispuesto por los artículos 55, 56, 124, párrafo segundo, y 125, fracción I, de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Campeche.

II. GLOSARIO

1. **ARCO:** Acceso, rectificación, cancelación y oposición;

2. **COTAIPEC:** Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche;

3. **LPDPPSOEC:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche;

4. **LTAIPEC:** Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche;

5. **Sistema de tratamiento y/o Base de datos personales:** conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

6. **Soporte electrónico**: Son los medios de almacenamiento inteligibles sólo 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) y demás medios de almacenamiento masivo no volátil;

7. **Soporte físico:** Son los medios de almacenamiento inteligibles a simple vista, como por ejemplo, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, entre otros;

8. **Tratamiento:** cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas, 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, transferencia y, en general, cualquier uso o disposición de datos personales.

III. NOMBRE DE LOS SISTEMAS DE TRATAMIENTO O BASE DE DATOS PERSONALES Y EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR.

Nombre de los sistemas de tratamiento o base de datos personales	*Nombre, cargo y adscripción del administrador*
1. Acciones de capacitación a Sujetos Obligados. ***2.* Promoción de la cultura de Transparencia.**	Mtro. Leonardo Tomas Acuña Notario, nivel 5.1, Director de Capacitación y Promoción.
3. Denuncias en materia de protección de datos personales. **4. Recursos de revisión en materia de protección de datos personales.** ***5.* Solicitudes de ejercicio de derechos ARCO.**	M.A.P Mónica del Carmen Casanova Mena, nivel 5.2, Directora de Protección de Datos Personales.
***6.* Recursos de Revisión en materia de acceso a la información.**	Lic. Luis Miguel Rosado Lavalle, nivel 4.2, Titular de la Unidad de Asuntos Jurídicos.
7. Recursos Humanos. **8. Video-Vigilancia de la COTAIPEC.**	C.P. Nicte Che Castillo, 5.1, Director de Administración y Finanzas.
9. Sistema de Evolución Patrimonial, de Declaración de	C.P. José Esteban Bautista Zamora, nivel 4.1, Titular del Órgano Interno de Control.

Nombre de los sistemas de tratamiento o base de datos personales	*Nombre, cargo y adscripción del administrador*
Intereses y Constancias de Presentación de Declaración Fiscal.	
***10.* Eventos de la COTAIPEC.**	Lic. Rafael Ricardo Alcalá Campos, nivel 6., Titular de Comunicación Social.
11. Ejercicio Local de Gobierno Abierto. **12. Eventos de Gobierno Abierto.**	Nivel 5.1, Directora de Gobierno Abierto y Vinculación.
13. Denuncias por Incumplimiento a las obligaciones de transparencia.	Licda. Gabriela Ortiz Gutiérrez, nivel 5.1, Directora de Coordinación y Vigilancia de Sujetos Obligados.
***14.* Solicitudes de Información.**	Licda. Jennipher Betzaida Pech Dzib, nivel 7.3, Titular de la Unidad de Transparencia.

IV. FUNCIONES Y OBLIGACIONES DEL RESPONSABLE, ENCARGADOS Y TODAS LAS PERSONAS QUE TRATEN DATOS PERSONALES.

Sistema de tratamiento y/o base de datos personales	***Funciones y obligaciones***
1. Acciones de capacitación a Sujetos Obligados.	Realizar el registro de los participantes en las acciones de capacitación, validar la asistencia a los cursos, brindar la capacitación, generar las constancias respectivas, elaborar informes y, en su caso, establecer comunicación con dichos participantes.
2. Promoción de la cultura de Transparencia.	Realizar el registro de los participantes en las acciones de promoción de la cultura de la transparencia, acceso a la información pública y protección de datos personales dirigidas a los habitantes del Estado de Campeche.
3. Denuncias en materia de protección de datos personales.	Recibir, registrar y tramitar denuncias en materia de protección de datos personales en posesión de sujetos obligados, de conformidad con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.
4. Recursos de revisión en materia de protección de datos personales.	Registrar, sustanciar y notificar los acuerdos y determinaciones que la Comisión tome para atender los recursos de revisión que usted presente, contra actos o resoluciones de los responsables en materia de protección de datos personales.
5. Solicitudes de ejercicio de derechos ARCO.	Dar atención a las solicitudes de ejercicio de derechos ARCO que se presenten ante la COTAIPEC, como responsable del tratamiento de los datos personales.
6. Recursos de revisión en materia de acceso a la información.	Registrar, sustanciar y notificar los acuerdos y determinaciones que la Comisión tome para atender los recursos de revisión que se interpongan contra actos o resoluciones de los sujetos obligados en materia de acceso a la información.
7. Recursos Humanos.	Integración de expedientes personales de cada uno de los empleados que laboran en la Comisión, así como la administración de nómina, pago de impuestos, prestaciones y cuotas, revisión de auditorías, cumplimiento de obligaciones laborales ante otras autoridades (IMSS, INFONAVIT, etc), y movimientos de personal.
8. Video-Vigilancia de la COTAIPEC.	Preservar la seguridad de las personas y las instalaciones de la COTAIPEC.

9. Sistema de Evolución Patrimonial, de Declaración de Intereses y Constancias de Presentación de Declaración Fiscal.	Mantener actualizada la base de datos personales denominada el Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal de los Servidores Públicos que ingresen, estén en activo o causen baja en la COTAIPEC.
10. Eventos de la COTAIPEC.	Promover y difundir el conocimiento en las materias que son de competencia de la Comisión, recabar las imágenes, videos y audios en los seminarios, cursos, talleres, capacitaciones, concursos, sesiones, eventos y otros foros que realice la Comisión; para su difusión en la página de internet de la Comisión, sus redes sociales y en los informes que realice para rendir cuentas de sus actividades.
11. Ejercicio Local de Gobierno Abierto.	Integrar el registro de interesados en participar en el ejercicio de gobierno abierto en Campeche y contactar a los interesados con el fin de interactuar, entablar diálogo o intercambiar opiniones respecto a las propuestas remitidas por los mismos.
12. Concurso infantil "Hablemos de Trasparencia y Privacidad" y el Concurso Juvenil de Cartel "Protege tus Datos Personales en las Redes Sociales”.	Cumplir con lo establecido en las bases del Primer Concurso Infantil "Hablemos de Trasparencia y Privacidad" y el Concurso Juvenil de Cartel "Protege tus Datos Personales en las Redes Sociales" integrar el registro de concursantes, identificar y mantener el contacto con los participantes para el resultado del concurso y publicar el nombre de los ganadores.
13. Denuncias por Incumplimiento a las obligaciones de transparencia.	Recibir, registrar y tramitar las denuncias derivadas del incumplimiento a las obligaciones de transparencia, recibidas vía Plataforma Nacional de Transparencia (http://www.plataformadetransparencia.org.mx/), correo electrónico (denuncia@cotaipec.org.mx) o, bien, por escrito presentado físicamente ante la Unidad de Transparencia de la Comisión.
14. Solicitudes de Información.	Recibir y dar trámite a las solicitudes de acceso a la información.

V. INVENTARIO DE DATOS PERSONALES TRATADOS EN CADA SISTEMA DE TRATAMIENTO Y/O BASE DE DATOS PERSONALES.

Nombre de los sistemas de tratamiento o base de datos personales	***Categorías de datos personales***	***Datos personales***	***Fundamento legal***
1. Acciones de capacitación a Sujetos Obligados.	Datos de identidad	• Nombre completo • Género • Firma	*Artículo 33 fracción IX de la LTAIPEC.* *Articulo 128 fracciones XXI y XXIII de la LPDPPSOEC.* *Artículo 43 fracción II del Reglamento Interior de la COTAIPEC.*
	Datos laborales	• Puesto • Correo electrónico institucional • Nombre del Sujeto • Obligado al que pertenecen	
2. Promoción de la cultura de Transparencia.	Datos de identidad	• Nombre completo • Género • Firma (en su caso)	Artículo 58 párrafo segundo de la LTAIPEC. Artículo 43 fracción II del Reglamento Interior de la COTAIPEC.
3. Denuncias en materia de protección de datos personales.	Datos de identidad	• Nombre • Domicilio • Firma	Artículos 160, 161 fracciones II y 162 de la LPDPPSOEC.
	Datos biométricos	• Huella dactilar	

4. Recursos de revisión en materia de protección de datos personales.	Datos de identidad	• Nombre del recurrente, representante o tercero interesado • Domicilio • Firma	Artículo 128 fracción IV de la LPDPPSOEC Artículo 46 fracción V del Reglamento Interior de la COTAIPEC.
	Datos electrónicos	• Correo electrónico personal	
5. Solicitudes de ejercicio de derechos ARCO.	Datos de identidad	• Nombre del titular o representante • Domicilio • Identificación oficial	Artículos 73, 76, 78, 82 y 117 de la LPDPPSOEC.
	Datos electrónicos	• Correo electrónico personal	
6. Recursos de revisión en materia de acceso a la información.	Datos de identidad	• Nombre • Domicilio particular • Firma	Artículos 149 y 159 de la LTAIPEC -Artículo 41 fracción I del Reglamento Interior de la COTAIPEC
	Datos electrónicos	• Correo electrónico	
7. Recursos Humanos.	Datos de identidad	• Nombre completo • Domicilio particular • Firma • Registro Federal de contribuyentes (RFC)	Artículo 42 fracción VI del Reglamento Interior de la COTAIPEC. Artículo 32 de las Condiciones Generales de Trabajo de la COTAIPEC.
	Datos electrónicos	• Correo electrónico personal	

	Datos laborales	• Nombramientos • Incidencias • Capacitaciones • Actividades extracurriculares	
	Datos patrimoniales	• Información fiscal	
	Datos académicos	• Título profesional • Cédula profesional • Certificados • Reconocimientos	
	Datos afectivos y/o familiares	• Número de dependientes	
8. Video-Vigilancia de la COTAIPEC.	Datos de identidad	• Imagen	Artículo 42 fracción VIII del Reglamento Interior de la COTAIPEC.
9. Sistema de Evolución Patrimonial, de Declaración de Intereses y Constancias de Presentación de Declaración Fiscal.	Datos de identidad	• Nombre completo • Domicilio particular • Teléfono particular • Teléfono celular personal • Firma • Clave de Registro Federal de contribuyentes (RFC) • Clave Única de Registro de Población (CURP)	Artículo 50 del Reglamento Interior de la COTAIPEC. Artículos 29 y 31 de la Ley General de Responsabilidades Administrativas.

		• Lugar y fecha de nacimiento • Género • Nacionalidad • Edad	
	Datos electrónicos	• Correo electrónico	
	Datos patrimoniales	• Bienes muebles e inmuebles • Información fiscal • Ingresos y egresos • Cuentas bancarias	
	Datos afectivos y/o familiares	• Estado civil • Dependientes económicos	
10. Eventos de la COTAIPEC.	Datos de identidad	• Imagen • Audio • Video	Articulo 48 fracciones IX y X del Reglamento Interior de la COTAIPEC.
11. Ejercicio Local de Gobierno Abierto.	Datos de identidad	• Nombre completo • Número telefónico	Artículo 45 fracciones II y IV del Reglamento Interior de la COTAIPEC.
	Datos electrónicos	• Correo electrónico	
	Datos laborales	• Institución de procedencia	
12. Eventos de Gobierno Abierto	Datos de identidad	• Nombre completo • Número telefónico	Artículo 45 fracción V del Reglamento Interior de la COTAIPEC.
	Datos electrónicos	• Correo electrónico	
	Datos laborales	• Institución de procedencia	

13. Denuncias por Incumplimiento a las obligaciones de transparencia.	Datos de identidad	• Nombre completo • Domicilio	Artículos 93, 95 y 98 de la LTAIPEC. Artículo 44 fracción II del Reglamento Interior de la COTAIPEC.
	Datos electrónicos	• Correo electrónico	
14. Solicitudes de Información.	Datos de identidad	• Nombre completo • Domicilio	Artículo 51 fracción II de la LTAIPEC.
	Datos electrónicos	• Correo electrónico	

VI. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO Y/O BASES DE DATOS PERSONALES SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Nombre de los sistemas de tratamiento o base de datos personales	*Tipo de Soporte*	*Características del lugar de resguardo*	*Programas en los que se utilizan los Datos Personales*
1. Acciones de capacitación a Sujetos Obligados.	Físico: Documentos y expedientes Electrónico: Base de datos	Físico: Av. Héroes de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta baja. Dirección de Capacitación y Promoción. Archivero puza 1 de 3 cajones, cajón 1. Electrónico: Computadora de escritorio marca ACER, modelo ASPIRE XC - 710	Paquetería Office: Word, Excel, power point
2. Promoción de la cultura de Transparencia.	Físico: Documentos y expedientes	Físico: Av. Héroes de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta baja. Dirección de Capacitación y Promoción. Archivero puza 2 de 3 cajones, cajón 2.	Paquetería Office: Word, Excel, power point
3. Denuncias en materia de protección de	Físico: Documentos y expedientes	Físico: Av. Héroes de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta baja. Dirección de Protección de Datos Personales, primer cubículo	Paquetería office: Word y Power point

datos personales.	Electrónico: Correo electrónico	de aproximadamente de 2.50 por 2.50 metros. Archivero puza de 3 cajones, específicamente en el cajón No. 1. Electrónico: Computadora de escritorio marca ACER modelo ASPIRE XC-710 y computadora de escritorio marca DELL, modelo D11S	
4. Recursos de revisión en materia de protección de datos personales.	Físico: Documentos y expedientes Electrónico: Base de datos y plataforma nacional de transparencia	Físico: Av. Héroes de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta baja. Dirección de Protección de Datos Personales, primer cubículo de aproximadamente de 2.50 por 2.50 metros. Archivero puza de 3 cajones, específicamente cajón No. 1. Electrónico: Computadora de escritorio marca ACER modelo ASPIRE XC-710 y computadora de escritorio marca DELL, modelo D11S.	Paquetería office: Word, Power point, Excel.
5. Solicitudes de ejercicio de derechos ARCO.	Físico: Documentos y expedientes Electrónico: Correo electrónico, PNT	Físico: Av. Héroes de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta baja. Dirección de Protección de Datos Personales, primer cubículo de aproximadamente de 2.50 por 2.50 metros. Archivero puza de 3 cajones, específicamente en el cajón No. 1. Electrónico: Computadora de escritorio marca ACER modelo ASPIRE XC-710 y computadora de escritorio marca DELL, modelo D11S.	Paquetería office: Word, Excel, PDF

6. Recursos de revisión en materia de acceso a la información.	Físico: Documentos y expedientes Electrónico: Base de datos y Plataforma Nacional de Transparencia	Físico: Av. Héroe de Nacozari No. 220, Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta alta. Unidad de Asuntos Jurídicos, cubículo privado y completamente cerrado de aproximadamente de 5.00 por 5.00 metros. Dos archiveros Maple de 3 gavetas cada uno. Electrónico: Computadora de escritorio marca Dell modelo Vostro y en el Sistema de Comunicación con Sujetos Obligados de la Plataforma Nacional de Transparencia https://www.plataformadetransparencia.org.mx/, con usuario asignado al organismo garante del Estado de Campeche.	Paquetería office: Word y Power point; Adobe Acrobat DC; funcionalidades de la Plataforma Nacional de Transparencia.
7. Recursos Humanos.	Físico: Documentos y expedientes Electrónico: Base de datos, Sistema COMPAQ, SUA y Plataforma Nacional de Transparencia	Físico: Av. Héroes de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta alta. Dirección de Administración y Finanzas de aproximadamente 2.50 por 2.50 metros. Archivero 3 cajones, específicamente en cajones No. 3. Electrónico: Computadora de escritorio marca Dell Optiplex 3080 micro, Intel core I 5-10500T, 16 GB DDR4, con WINDOWS 10 PRO, monitor DELL 210-AQDX 24" modelo P2419H No. serie: CN-0GMGXF-TV200-05H-13LT-A09. Sistema COMPAQ, SUA y link de Plataforma Nacional de Transparencia: https://www.plataformadetransparencia.org.mx/web/guest/inicio	Paquetería office: Word y Power point
8. Video-Vigilancia de la COTAIPEC.			

9. Sistema de Evolución Patrimonial, de Declaración de Intereses y Constancias de Presentación de Declaración Fiscal.	Físico: Formato de declaración patrimonial autorizado	Físico: Av. Héroes de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta baja. Órgano Interno de Control, oficina junto al Comisionado Presidente de 3x3 mts2. Archivero línea Italia de 3 cajones, la documentación se encuentra en el cajón 1.	Paquetería office: Excel
10. Eventos de la COTAIPEC.			
11. Ejercicio Local de Gobierno Abierto.	Físico: Documentos y expedientes	Físico: Av. Héroes de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta alta. Dirección de Gobierno Abierto y Vinculación, primer cubículo de aproximadamente de 4.00 por 2.50 metros. Archivero No. 1, específicamente cajón No. 2.	Paquetería office: Word
12. Eventos de Gobierno Abierto	Físico: Documentos y expedientes Electrónico: Redes sociales de Facebook, Twitter, YouTube y pagina WEB	Físico: Av. Héroes de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo; Planta alta, Departamento de Comunicación Social, archivero línea italika de 5 cajones con resguardo a mi nombre 5111000002-2, específicamente esta información se encuentra marcado cajón 2, comunicación social, archivero fotográfico, audioteca y videoteca". Electrónico: Computadora portátil marca Dell, inspiron 15 5000, serie 9C76XF2	En media player y herramientas de pre visualización de imágenes y audio de Windows.

	de la COTAIPEC		
13. Denuncias por Incumplimiento a las obligaciones de transparencia.	Físico: Documentos y expedientes Electrónico: Correo electrónico	Físico: Av. Héroes de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta alta. Dirección de Coordinación y Vigilancia de Sujetos Obligados, cubículo ubicado en la Dirección, cerrado con puerta de madera, aproximadamente de 3 metros de largo por 1.20 de ancho. Archivero CRISA de 3 cajones con llave. Electrónico: Computadora de escritorio marca Dell modelo D14U con número de serie 925QV63. Mediante el correo electrónico denunicas@cotaipec.org.mx	Paquetería office: Word
14. Solicitudes de Información.	Físico: Documentos y expedientes Electrónico: Expedientes electrónicos, SISAI	Físico: Av. Héroe de Nacozari No. 220. Col. Ampliación Cuatro Caminos, entre calle Tacubaya y Av. López Portillo. Planta baja. Unidad de Transparencia, cubículo del lado izquierdo de aproximadamente de 3.00 por 2.50 metros. Archivero puza 3 cajones específicamente esta información se encuentra en los cajones marcados con los No. 1,2.y 3 Electrónico: computadoras de escritorio marca Dell modelos VOSTRO3471 y D14U http://www.plataforma de trasparencia.campeche.org.mx	Paquetería office: Word, Excel, PDF

VII. CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS QUE, EN SU CASO, SE EFECTÚEN.

Transmisiones mediante el traslado de soportes físicos	El envío se realiza a través del personal adscrito a las ponencias, a la Secretaría Ejecutiva o mediante personal autorizado por su superior jerárquico y con oficio de comisión y/o permiso; Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas; La información sólo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial; Toda entrega de información requiere acuse de recibo, y A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área.

Transmisiones mediante el traslado físico de soportes electrónicos	El envío se realiza a través del personal adscrito a las ponencias, a la Secretaría Ejecutiva mediante personal autorizado por su superior jerárquico y con oficio de comisión y/o permiso; Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas; La información sólo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial; Toda entrega de información requiere acuse de recibo, y A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área; A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán estar cifrados.
Transmisiones mediante el traslado sobre redes electrónicas	El envío se realiza a través del Personal adscrito a las Ponencias, a la Secretaría Ejecutiva o mediante personal autorizado por su superior jerárquico y únicamente a través de medios electrónicos institucionales.

**(Formato 2 de los anexos)*

VIII. RESGUARDO DE LOS SOPORTES FÍSICOS Y/O ELECTRÓNICOS DE LOS DATOS PERSONALES

a) Resguardo físico

EQUIPO	BAJO RESGUARDO	CARGO	MARCA	MODELO	SERIE
DIRECCIÓN DE COORDINACIÓN Y VIGILANCIA DE SUJETOS OBLIGADOS					
Archivero 3 cajones	Gabriela Ortiz Gutiérrez	Directora	PUZA	TRIPLAY	ARCH3GAV
Archivero móvil	Gabriela Ortiz Gutiérrez	Directora	CRISA	106	S/N
Archivero móvil	Francisco Javier Pech Rosado	Jefe de Departamento	CRISA	106	S/N
Archivero móvil	Mauricio Preve Grajales	Jefe de Departamento	CRISA 3 GAV	106XL	S/N
Archivero móvil	Mauricio Preve Grajales	Jefe de Departamento	CRISA	106XL	S/N
Archivero móvil	Ricardo Manuel Chi Gallardo	Jefe de Departamento	CRISA	106	S/N
DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS					
Archivero 3 cajones	Nicte Che Castillo	Directora	SIMMEX	AV3	S/N
Archivero móvil	Nicte Che Castillo	Directora	CRISA	106XL	S/N
Archivero	Manuel Fernando Olea Montero	Jefe de Departamento	PUZA	TRIPLAY	ARCH2GAV
Archivero móvil	Manuel Fernando Olea Montero	Jefe de Departamento	CRISA	106XL 3 CAJONES	S/N
Archivero	Jhosefyne Jasmin Arteaga Puch	Jefe de Departamento	PUZA	TRIPLAY	ARCH2GAV
Archivero	Juan Enrique Estrella Medina	Analista	PUZA	TRIPLAY	ARCH2GAV

DEPARTAMENTO DE COMUNICACIÓN SOCIAL					
Archivero de Triplay	Rafael Ricardo Alcalá Campos	Jefe de Departamento	CRISA	S/N	S/N
Archivero de Triplay	Rafael Ricardo Alcalá Campos	Jefe de Departamento	CRISA	S/N	S/N
Archivero móvil	Rafael Ricardo Alcalá Campos	Jefe de Departamento	CRISA	106	S/N
UNIDAD DE ASUNTOS JURÍDICOS					
Archivero móvil	Luis Miguel Rosado Lavalle	Director	CRISA	106	S/N
Archivero móvil	Luis Miguel Rosado Lavalle	Director	Maple	3 GAVETAS	S/N
Archivero móvil	Luis Miguel Rosado Lavalle	Director	Maple	3 GAVETAS	S/N
Archivero móvil	Luis Miguel Rosado Lavalle	Director	CRISA	106	S/N
Gabinete par archivo	Luis Miguel Rosado Lavalle	Director	PUZA	TRIPLAY	GAB3ENT
Archivero de metal	Cecilia Faride López Pérez	Jefe de Departamento	ITALIA	S/N	S/N
Archivero móvil	Lourdes Guadalupe Dzib Haaz	Jefe de Departamento	CRISA	106	S/N
Archivero móvil	León Alberto Montero Jiménez	Analista	S/N	S/N	S/N
DIRECCIÓN DE CAPACITACIÓN Y PROMOCIÓN					
Archivero móvil	Leonardo Tomás Acuña Notario	Director	CRISA	106XL	S/N
Archivero móvil	Leonardo Tomás Acuña Notario	Director	CRISA	106XL	S/N
Archivero móvil	Leonardo Tomás Acuña Notario	Director	CRISA	106	S/N

Gabinete par archivo	Leonardo Tomás Acuña Notario	Director	CRISA	302	S/N
Archivero móvil	Víctor Hugo Osorio Colli	Analista	CRISA	106	SN
Archivero móvil	Limberth Andrés Balam Dzib	Analista	CRISA	106	S/N
Archivero móvil	Emma Yaneth Fernández Cu	Analista	CRISA	106	SN
ÓRGANO INTERNO DE CONTROL					
Archivero	José Esteban Bautista Zamora	Contralor	QUATTRA	ITALIA	S/N
Archivero móvil	José Esteban Bautista Zamora	Contralor	CRISA	ITALIA	S/N
Archivero móvil	José Esteban Bautista Zamora	Contralor	QUATTRA	S/N	S/N
DIRECCIÓN DE PROTECCIÓN DE DATOS PERSONALES					
Archivero	Mónica del Carmen Casanova Mena	Director	SIMMEX	AF3-A	S/N
Archivero móvil	Amy Abigaíl Osorno Sosa	Analista	SIMMEX	AM1	S/N
Archivero 3 cajones	Raciel Adalio Quiñones Flores	Analista	PUZA	TRIPLAY	ARCH3GAV
Archivero móvil	Raciel Adalio Quiñones Flores	Analista	SIMMEX	AM1	S/N
DIRECCIÓN DE GOBIERNO ABIERTO					
Archivero 3 cajones	María Isabel Márquez Martínez	Jefe de Departamento	S/N	3 GAVETAS	S/N
Archivero de triplay	María Isabel Márquez Martínez	Jefe de Departamento	CRISA	S/N	S/N
Archivero móvil	Juan Carlos Ake Villareal	Jefe de Departamento	CRISA	106	S/N

UNIDAD DE TRANSPARENCIA					
Archivero 3 cajones	Jenipher Betzaida Pech Dzib	Jefe de Departamento	PUZA	TRIPLAY	ARCH3GAV
Archivero móvil	Jenipher Betzaida Pech Dzib	Jefe de Departamento	CRISA	106	S/N
Archivero móvil	Eric Yanuario Castillo Trejo	Analista	CRISA	106	S/N

b) **Resguardo electrónico**

EQUIPO	BAJO RESGUARDO	CARGO	MARCA	MODELO	SERIE
DIRECCIÓN DE COORDINACIÓN Y VIGILANCIA DE SUJETOS OBLIGADOS					
Computadora de escritorio	Gabriela Ortiz Gutiérrez	Directora	DELL	D14U	925QV63
Computadora portátil Laptop	Francisco Javier Pech Rosado	Jefe de Departamento	DELL	VOSTRO 14	9R1LSJ2
Microcomputadora portátil Laptop	Mauricio Preve Grajales	Jefe de Departamento	HP	RTL8723BE	6EZRU09WY424MU
Microcomputadora portátil Laptop	Ricardo Manuel Chi Gallardo	Jefe de Departamento	DELL	DELL INSPIRON 15	TTYFJA00
Computadora portátil Laptop	Erick Raymundo Zabala Pérez	Jefe de Departamento	DELL	VOSTRO 3468	G52LSJ2

Computadora portátil Laptop	Alejandra Isabel Panti Panti	Analista	HP	15-da0089lm LTNA	CND921716K
DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS					
Computadora de escritorio	Nicte Che Castillo	Directora	DELL	OptiPlex	B3FRXG2
Computadora de escritorio	Manuel Fernando Olea Montero	Jefe de Departamento	DELL	D14U	33BQV63
Procesador de computadora	Jhosefyne Jasmin Arteaga Puch	Jefe de Departamento	DELL	VOSTRO	D24VJK2
Computadora de escritorio	Elisa de Jesús Wong Dorantes	Analista	INSPIRON	3268	43302262646
Computadora de escritorio	Juan Enrique Estrella Medina	Analista	ACER	ASPIRE XC-710	DTB16AL007624008E13000
Unidad Central de Procesos (CPU)	Pedro José López Nieves	Analista	DELL	VOSTRO 3474	B2WK013
DEPARTAMENTO DE COMUNICACIÓN SOCIAL					
Computadora de escritorio	Rafael Ricardo Alcalá Campos	Jefe de Departamento	APPLE	A1418	C02NHG43FY0T
Computadora portátil Laptop	Rafael Ricardo Alcalá Campos	Jefe de Departamento	DELL	Inspiron 15 5000	9C76XF2
Microcomputadora portátil Laptop	Rafael Ricardo Alcalá Campos	Jefe de Departamento	HP	PROBOOK	CNU126459S

UNIDAD DE ASUNTOS JURÍDICOS					
Computadora de escritorio	Luis Miguel Rosado Lavalle	Director	ACER	ASPIRE XC-710	DTB16AL0076240094C3000
Computadora de escritorio	Luis Miguel Rosado Lavalle	Director	ACER	ASPIRE XC-713	DTB16AL007624009933000
Computadora de escritorio	Luis Miguel Rosado Lavalle	Director	LENOVO	AIO-330201GM	YJ00RA9F
Unidad Central de Procesos (CPU)	Luis Miguel Rosado Lavalle	Director	DELL	VOSTRO 3472	71XR333
Computadora de escritorio	Cecilia Faride López Pérez	Jefe de Departamento	DELL	D11S	5NNR333
Unidad Central de Procesos (CPU)	Lourdes Guadalupe Dzib Haaz	Jefe de Departamento	DELL	VOSTRO 3473	H5D9933
Computadora de escritorio	León Alberto Montero Jiménez	Analista	ACER	ASPIRE XC-714	DTB16AL007624009533000
DIRECCIÓN DE CAPACITACIÓN Y PROMOCIÓN					
Computadora de escritorio	Leonardo Tomás Acuña Notario	Director	ACER	VX5E1 VERITION	DTVPUAL003732052BF9600
Computadora portátil Laptop	Leonardo Tomás Acuña Notario	Director	DELL	VOSTRO 3468	J12LSJ2
Unidad Central de Procesos (CPU)	Víctor Hugo Osorio Colli	Analista	LENOVO	10SU-S1RP00	MJ08K5PZ

Computadora de escritorio	Limberth Andrés Balam Dzib	Analista	DELL	D11S	CZFYN23
Computadora de escritorio	Diosaleth Rosado Gómez	Analista	ACER	ASPIRE	44200403563
Computadora de escritorio	Emma Yaneth Fernández Cu	Analista	DELL	INSPIRON 3647	7XMW182
ÓRGANO INTERNO DE CONTROL					
Computadora de escritorio	José Esteban Bautista Zamora	Contralor	HP	AIO-24F111LA	SN
Computadora portátil Laptop	José Esteban Bautista Zamora	Contralor	DELL	VOSTRO 3480	2XDCB53
DIRECCIÓN DE PROTECCIÓN DE DATOS PERSONALES					
Computadora de escritorio	Mónica del Carmen Casanova Mena	Director	DELL	D11S	5NSRD33
Computadora de escritorio	Amy Abigaíl Osorno Sosa	Analista	ACER	ASPIRE XC-710	DTB16AL007624009B23000
Computadora de escritorio	Raciel Adalio Quiñones Flores	Analista	INSPIRON	3470	12058139126
DIRECCIÓN DE GOBIERNO ABIERTO					
Computadora portátil Laptop	María Isabel Márquez Martínez	Jefe de Departamento	DELL	VOSTRO 14	6S1LSJ2

Computadora de escritorio	María Isabel Márquez Martínez	Jefe de Departamento	DELL	D11S	5NPR333
Computadora de escritorio	Juan Carlos Ake Villareal	Jefe de Departamento	ACER	ASPIRE XC-712	DTB16AL007624008DB3000
UNIDAD DE TRANSPARENCIA					
Computadora de escritorio	Jenipher Betzaida Pech Dzib	Jefe de Departamento	DELL	D14U	505QV63
Unidad Central de Procesos (CPU)	Eric Yanuario Castillo Trejo	Analista	DELL	VOSTRO 3471	D390853

IX. BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Se utilizan bitácoras de acceso en soportes físicos únicamente en los casos en que personal ajeno a los responsables de los sistemas de tratamiento o base de datos personales requieran acceder a la información contenida en ellos, o bien, en los casos en los cuales tratándose de soportes físicos estos se encuentren en el archivo de concentración por haber fenecido su periodo de trámite, para lo cual se requerirá, además de la autorización del responsable del sistema de tratamiento o base de datos personales, la autorización del responsable del archivo de concentración, conforme a los procedimientos archivísticos establecidos.
Para los casos en que se requiera extraer algún equipo de cómputo o cualquier otro activo electrónico que contenga datos personales se deberá solicitar la autorización correspondiente mediante el llenado del FORMATO 1 contenido en los anexos.

Las bitácoras de acceso a los datos personales en soportes físicos deberán contener lo siguiente:

- Nombre y cargo de quien accede
- Área de adscripción
- Identificación del Expediente
- Fojas del Expediente
- Propósito del Acceso
- Fecha de Acceso
- Hora de Acceso
- Fecha de Devolución
- Hora de Devolución

*(*Formato No. 3 de los anexos).*

Las bitácoras de vulneraciones a la seguridad deberán contener lo siguiente:

- Fecha del incidente;
- Nombre y cargo;
- Área de adscripción:
- Responsable del área;
- Sistema de tratamiento o base de datos personales vulnerada;
- Cantidad de titulares vulnerados;
- Soporte de la información vulnerada;
- Tipo de vulneración;
- Tipo de dato personal afectado:
- Nombre y firma de quien reporta;
- Nombre y firma del administrador del sistema;

*(*Formato No. 4 de los anexos).*

X. ANÁLISIS DE RIESGOS

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPEC

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

[redacted]

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

- [redacted]
- [redacted]
- [redacted]

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

XI. ANÁLISIS DE BRECHA.

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

[redacted]

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

Eliminado Información Reservada. Art. 113. Fracción III. LTAIPE

[redacted]

XII. GESTIÓN DE VULNERACIONES

Plan de respuesta

- Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.
- En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes.
- Llenado de formato No. 4 (anexo), por parte de la persona que detectó la vulneración.
- Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.
- Elaboración de Informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia.
- Notificación a titulares en un lapso de 72 horas que de forma significativa vea afectados sus derechos patrimoniales o morales.
- Llenado de la bitácora de vulneraciones conforme al artículo 59 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

XIII. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

En términos del artículo 3 fracción XXV de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Campeche, las medidas de seguridad son un conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales, sujetos a tratamiento al interior del responsable, y de los que se transfieran o remitan por diversas vías, a saber, las medidas de seguridad que actualmente se aplican son las siguientes:

A. Medidas de seguridad físicas

Para garantizar la seguridad física de las instalaciones, personas y equipos de la institución se cuenta con cuenta procedimientos de control y prevención ante amenazas al entorno físico de los datos y de los recursos involucrados en su tratamiento, los cuales se describen a continuación:

	Medida	Finalidad	Descripción
Medidas de Seguridad físicas	Seguridad privada en edificio sede.	Prevenir el acceso no autorizado al perímetro de la organización. Prevenir el daño o interferencia a las instalaciones. Proteger los recursos móviles, portátiles y	Las instalaciones son resguardadas por un elemento (personal) de vigilancia privada, miembro de la persona moral con la que se tiene firmado contrato de prestación de tal servicio, en horas hábiles inicia a las 20:00 horas de cada día y termina a las 8:00 horas del día siguiente, y en días inhábiles las 24 horas del día.

		cualquier soporte físico o electrónico.	
	Instalación de cámaras de video vigilancia.	Prevenir el acceso no autorizado al perímetro de la organización. Prevenir el daño o interferencia a las instalaciones. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico.	Las instalaciones cuentan con sistema de video-vigilancia que consta de 8 cámaras ubicadas en sitios estratégicos o de acceso a las instalaciones.
	Barda perimetral	Prevenir el acceso no autorizado al perímetro de la organización. Prevenir el daño o interferencia a las instalaciones. Proteger los recursos móviles, portátiles y	Las instalaciones cuentan con barda perimetral de aproximadamente de 3 metros de altura que cubre la totalidad de las instalaciones, y cuentan con dos accesos, uno frontal sobre avenida Héroes de Nacozari y otro trasero sobre calle Tacubaya.

		cualquier soporte físico o electrónico.	
	Acceso a Unidades administrativas.	Prevenir el acceso no autorizado al perímetro de la organización. Prevenir el daño o interferencia a las instalaciones. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico.	Las unidades administrativas cuentan con puertas de acceso con cerraduras, las llaves se encuentran bajo resguardo del titular del área administrativa. Fuera del horario oficial de labores, salvo situaciones extraordinarias, las puertas de acceso a las unidades administrativas se deben mantener cerradas bajo llave.
	Seguridad física de equipos	Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico.	Los equipos de cómputo se sitúan sobre superficies fijas, mesas de trabajo y escritorios, a una altura adecuada para evitar caídas daños por estas. Los equipos de cómputo se ubican lejos de ventanas para evitar que objetos lanzados desde el exterior caigan sobre ellos y los dañen.

			Tanto los equipos de cómputo (soportes electrónicos) como archiveros (soportes físicos) cuentan el debido cuidado por parte del servidor público del cual se encuentran bajo resguardo. En las plantas alta y baja de las instalaciones se cuentan con extintores de incendios, conforme al plan interno de protección civil.

B. Medidas de seguridad técnicas

Para garantizar la seguridad técnica y operatividad de los recursos tecnológicos (hardware y software) involucrados en el tratamiento de datos personales se realizan e implementan las acciones y mecanismos siguientes:

	Medida	Finalidad	Descripción
Medidas de Seguridad Técnicas	Usuarios y contraseñas.	Prevenir que el acceso a los datos personales, así como a los recursos, sea por usuarios identificados y autorizados; Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.	Los equipos de cómputo asignados a cada servidor público para el desempeño de sus funciones, cuentan con contraseña de encendido y contraseña de usuario.

	Software de seguridad	Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.	Todos los equipos de cómputo cuentan con programas antivirus bajo licencia. Los registros de renovación de licencia o cambio de software corren a cargo de la Dirección de Tecnologías de la Información
	Mantenimiento de equipos.	Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.	Realizar de manera periódica el mantenimiento preventivo o, en su caso, correctivo de los equipos de cómputo en los cuales se tratan datos personales. Se lleva una bitácora de tales acciones a cargo de la Dirección de la Información

C. Medidas de Seguridad Administrativas

Para garantizar la seguridad administrativa de los datos personas en la gestión de los procesos a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales, así como la sensibilización y capacitación del personal en materia de protección de datos personales se toman las siguientes medidas:

	Medida	Finalidad	Descripción
Medidas de Seguridad Administrativas	Capacitación general y particular.	Sensibilizar y capacitar al personal en materia de protección de datos personales. Que el personal conozca y cumpla con los principios, deberes, derechos y demás obligaciones en la materia y las sanciones en caso de incumplimiento.	Todos los empleados deben recibir una capacitación sobre aspectos generales de la ley al menos una vez por año y los nuevos colaboradores en sus primeros 90 días de entrar en funciones, conforme al programa general de capacitación para la institución.

	Establecer Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales.	Delimitar las actuaciones en la gestión de los procedimientos internos. Establecer los principios que rigen el actuar de los servidores públicos de la Comisión.	Se cuentan con las disposiciones normativas siguientes: -Código de Conducta de los servidores públicos de la Comisión de Transparencia y Acceso a la Información Pública del estado de Campeche. -Manual de procedimientos de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche. -Manual de Procedimientos de Organización y Disposición Documental de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche.

XIV. CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Los servidores públicos trabajadores de la Comisión en todo momento deberán portar el uniforme y contar a su vez con gafetes identificativos, los cuales deberán de contener:

Al frente:	Al reverso:
• Nombre • Cargo • Fotografía • Área de adscripción	• Vigencia • Número de empleado • Firma del Presidente de la Comisión • Sitio oficial de internet • RFC de la Comisión • Domicilio institucional • Teléfono institucional

XV. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.

El respaldo de información es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica o un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

Los respaldos que se realicen de amanera periódica deberán registrarse en la bitácora de respaldos, que estará a cargo de la dirección de TI, conforme a lo marca el anexo (FORMATO 5).

XVI. PLAN DE CONTINGENCIA.

Es un conjunto de estrategias diseñadas para ser aplicadas, durante y luego de la presentación de una emergencia a fin de minimizar los daños que pueden ocasionarse tanto al personal a cargo como a la información. Estas medidas están incluidas en el Programa Interno de Protección Civil de la COTAIPEC, que estará sujeto para aprobación de la Secretaria de Protección Civil (SEPROCI), el cual implica un análisis de los posibles riesgos a los cuales puede estar expuesta nuestra información contenida en los diversos medios de almacenamiento de los sistemas de tratamiento o base de datos personales dependiendo del grado de emergencia.

a. Unidad Interna de Protección.

Se conformará la Unidad Interna de Protección Civil esta instancia será el primer contacto con los cuerpos de emergencia en las tareas de protección civil de la Comisión y la máxima autoridad en la materia al momento de presentarse un alto riesgo, emergencia, siniestro o desastre, el cual tendrá las siguientes funciones:

- Coordinar las acciones de protección civil en la comisión ante situaciones de riesgos y emergencias.
- Elaborar y coordinar el programa interno de protección civil.
- Difusión del documento una vez aprobado.
- Integrar la unidad interna de protección civil de la Comisión.
- Se debe contar con un responsable general quien guiará la implementación del mismo, así como la toma de las decisiones.
- Conformar las brigadas que conformaran la unidad interna de protección civil.
- Elaborar programas de actividades de capacitación y difusión.
- Identificar, analizar y evaluar riesgos internos y externos.
- Supervisar, elaborar y actualizar directorios de emergencias.
- Concertar acuerdos con autoridades fuera de las instalaciones.

- Promover la capacitación coordinando charlas sobre prevención, atención y recuperación de desastres para todo el personal involucrado en el proyecto.

b. Medidas de prevención y conservación de archivos

- Espacios con luz natural y sin humedad.
- Los muebles de archivo deben garantizar la conservación de los documentos que guardan; los documentos deben guardar uniformidad.
- Evitar archivar documentación cerca de aparatos eléctricos, las instalaciones eléctricas deben estar en buenas condiciones.
- Los estantes de los archivos deben de estar entre 10 y 15 cm del suelo (facilitan la limpieza y evita su vez la acumulación de humedad y proliferación de plagas).
- Todos los equipos eléctricos deben quedar apagados y desconectados durante la noche o cuando no se utilicen.
- Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.

c. Medidas preventivas ante siniestros

- ***Incendio:*** Si detecta un incendio procure mantener la calma y repórtelo inmediatamente a la brigada de prevención y combate de incendios para que atiendan la emergencia conforme a la planificación.

  Durante un incendio:
  - Si el incendio es pequeño, se procurará apagarlo mediante un extintor.
  - Si el fuego es de origen eléctrico no se deberá intentar apagarlo con agua.
  - No abra puertas ni ventanas el fuego se extiende con el aire.
  - Si el incendio no se puede controlar solicitar apoyo a los bomberos.
  - No pierda tiempo buscando objetos personales y salga del inmueble lo antes posible.

- Si hay gas o humo humedezca un trapo cubriendo nariz y boca.
- Si su ropa se enciende; tírese al piso y ruede lentamente.

Después del incendio:

- Mantener suspendida la corriente eléctrica, el agua y el gas hasta que se revise el estado del inmueble sus instalaciones y los servicios en general.
- Para regresar al interior del inmueble, es necesario que las personas responsables de Protección Civil otorguen la autorización y sea seguro.

Resguardo de la información en caso de incendio:

- Respaldo de información en una zona segura de preferencia, donde el calor de un incendio no alcance los dispositivos, esto es en lugares cercanos a los extintores (sugerencias para realizar el almacenamiento de la información: CD, Disco duro, dispositivos de almacenamiento, la nube únicamente si es segura).
- Tener identificados los documentos con mayor valor para resguardarlos en una zona segura (realizar la digitalización de los mismos con resguardo en la nube o dispositivos de almacenamiento).

- **Inundaciones:** Para evitar pérdidas graves es importante realizar la revisión y reparación de ventanas y puertas, por donde podría filtrarse el agua de lluvia, así como impermeabilizar los techos en temporada de lluvias esto para evitar goteras.

Previamente:

- Evitar colocar expedientes y/o documentos directamente sobre el piso.
- Respetar, al menos, una altura de 10 a 15 cm de los archiveros.
- Colocar barreras para el agua (cubrir los documentos de las goteras).
- Evacuar los documentos afectados hacia áreas ventiladas.

- Inmediatamente colocar papel secante en cada hoja de los expedientes.
- Si un documento en papel se moja en su totalidad se puede secar individualmente mediante ventilación o realizar la congelación del mismo para su recuperación, debe realizarlo preferentemente un especialista.

Durante una inundación:

- Desconectar servicios de luz, gas y agua.
- Mantenerse alejados de árboles y postes de luz.
- Evitar tocar o pisar cables eléctricos.
- Cubrir aparatos u objetos que puedan dañarse con el agua.

Después de la inundación:

- *Expulsar* el agua mediante esponjas, baldes, recogedores, en el caso de no contar con una bomba con motor de combustión.
- Cerciorarse de que los aparatos eléctricos estén secos antes de utilizarlos nuevamente.
- Desinfectar las áreas afectadas pisos, muros y mobiliario rescatable, con agua, jabón y cloro para evitar enfermedades.
- Ventilar las áreas afectadas después de la inundación.
- Identificar documentos dañados con la inundación y proceder a aplicar medidas para recuperarlo.
- Reportar lo que se dañó con el paso de la inundación.

- **Amenazas informáticas:** Ante un evento informático los pasos a seguir para mantener la seguridad de la información, son los siguientes:

  - Cambiar contraseñas.

- Las contraseñas no deben contener información personal como nombre real, nombre de usuario, fechas de nacimiento o incluso el nombre institucional.
- Deben ser muy distinta a tus contraseñas previas.

Para la atención ante una situación de emergencia de este tipo se utilizarán los siguientes elementos:

1. Brigada de prevención y combate de incendios: Intervendrán con los medios disponibles para tratar de evitar que se produzcan daños y pérdidas en las instalaciones de la comisión como consecuencia de una amenaza de incendio.

2. Sistema de alarma: Se ubicarán alarmas en lugares estratégicos, las cuales advertirán al personal la presencia de un peligro.

3. Detectores de Humo: Se ubicará en el archivo de concentración e histórico.

4. Equipos contra incendios: En las instalaciones se dispondrán y ubicarán extintores en un lugar visible y de fácil acceso.

5. Se deberá tener acceso al botiquín para realizar tratamientos de primeros auxilios.

6. La brigada de prevención y combate de incendios se encargará del manejo de los extintores, supervisará el mantenimiento de equipos contra incendio y será el personal capacitado para esta emergencia.

7. Mientras se está conectado a Internet el atacante tendrá acceso a los archivos e información guardados en la computadora vulnerada, por lo que recomienda desconectar el cable de la red lo antes posible.

XVII. TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

Los Métodos Físicos	*Trituración:* Mediante una máquina trituradora se cortará cada uno de los documentos de forma vertical, lo cual hace prácticamente imposible que se puedan unir. *Destrucción de los medios de almacenamiento electrónicos mediante desintegración:* separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.
Métodos lógicos	*Sobre-escritura*: escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes.

XVIII. PLAN DE TRABAJO.

De las medidas de seguridad faltantes por implementar se realizará un análisis para determinar el tiempo promedio para ser subsanadas, dicho periodo no podrá ser mayor a 24 meses una vez aprobado el presente documento de seguridad, tales adecuaciones se sujetaran, en el caso que requerir la erogación de recursos económicos, a las previsiones presupuestarias existentes, las medidas que no requieran la erogación de recursos deberán ser implementadas a partir de la aprobación del presente documento de seguridad y la vigilancia de su debida observancia estarán a cargo del Comité de Transparencia, la Dirección de Protección de Datos Personales y la Unidad de Transparencia, para lo que todas las áreas administrativas de la Comisión deberán prestarles las facilidades necesarias para implementación, vigilancia y evaluación de las medidas de seguridad implementadas y de las necesarias por implementar al interior de la institución.

XIX. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Informe anual	Se realizará un informe detallado de las medidas de seguridad existentes de manera anual por parte de la Dirección de Datos Personales, informando al Comité de Transparencia el estado que éstas guardan, durante el mes de enero de cada año.

XX. PROGRAMA GENERAL DE CAPACITACIÓN.

El programa de capacitación actualiza a los servidores públicos de los responsables y de la propia Comisión, en materia de Protección de Datos Personales, de conformidad con lo establecido por la Ley de Protección de Datos personales en Posesión de Sujetos Obligados del Estado de Campeche.

Estrategias de capacitación	
Capacitación permanente	Ofrecer cursos sobre aspectos generales de la Ley de Protección de Datos Posesión de Sujetos Obligados del Estado de Campeche.
Capacitación focalizada	Se impartirá el curso de los Lineamientos para la Protección de Datos Posesión de Sujetos Obligados del Estado de Campeche; y el curso sobre obligaciones de la Comisión como responsable.

Acciones de capacitación a responsables de tratamiento	
Proporciona a los servidores públicos las herramientas necesarias que les permitan mejorar la gestión de la protección de datos personales a fin de incrementar los niveles de seguridad en el tratamiento de datos personales al interior de la institución.	
Impartido por: Dirección de Protección de Datos Personales. *Dirigida a:* Integrantes del Comité de Transparencia, Titulares de las unidades administrativas, y cualquier otro personal involucrado en el tratamiento de datos personales al interior de la institución.	*Curso:* Aspectos Generales de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados. Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche. *Curso taller:* Derechos ARCO. *Taller:* Documento de seguridad y Aviso de Privacidad. *Conferencia:* Protección de Datos Personales en Redes Sociales

ANEXOS

FORMATO NO. 1

VALE DE INGRESO/SALIDA DE EQUIPOS DE CÓMPUTO

Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche

COTAIPEC

	No. de folio:	*Fecha:*
Nombre y cargo del Solicitante		
Área de adscripción		

Descripción del equipo	*Marca*	*Modelo*	*Serie*	*No. de inventario*

Salida del equipo de cómputo

Fecha: _____ *Hora:* _____

El bien es propiedad de la Comisión: Si ☐ No ☐

Nombre del responsable del equipo: _____

Motivo del préstamo: Reparación ☐ Comisión ☐ Otro: _____

Tiempo aproximado del préstamo: _____

_____ Firma del solicitante

_____ Firma del responsable del equipo

Devolucion del equipo de computo

Fecha: _____ *Hora:* _____

Descripción del equipo

_____

_____ Firma del solicitante

_____ Firma del responsable del equipo

FORMATO NO. 2

BITÁCORA DE TRANSFERENCIAS

Fecha	*Medio*	*Datos Personales Transferidos*	*Receptor*	*Persona que recibe*	*Autorización*

FORMATO No. 3

BITÁCORA DE ACCESO

Bitácora de Acceso						
Nombre y cargo de quien accede	Área de adscripción	Identificación del Expediente	Fojas del Expediente	Propósito del Acceso	Fecha y hora de Acceso.	Fecha y hora de Devolución.

FORMATO No. 4

VULNERACIONES A LA SEGURIDAD DE DATOS PERSONALES

Vulneraciones a la seguridad de datos personales	
Fecha del incidente	
Nombre y cargo	
Área de adscripción	
Responsable del área	
Sistema de tratamiento o base de datos personales vulnerada	
Cantidad de titulares vulnerados	
Soporte de la información vulnerada	Físico ☐ Electrónico ☐ Ambos ☐
Tipo de vulneración	☐ Pérdida o destrucción no autorizada ☐ Robo, extravío o copia no autorizada ☐ Uso, acceso o tratamiento no autorizado ☐ Daño, alteración o modificación no autorizada
Tipo de dato personal afectado	☐ Identidad ☐ Académicos ☐ Electrónico ☐ Laboral ☐ Patrimonial ☐ Salud ☐ Procedimientos administrativos o jurisdiccionales ☐ Tránsito y movimientos migratorios ☐ Biométricos ☐ Naturaleza pública ☐ Afectivos y/o familiares

_____ **Nombre y firma de quien reporta**	_____ **Nombre y firma del administrador del sistema**

FORMATO No. 5

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

ÁREA:		EQUIPO:	
		SERIE:	

Nombre y cargo del responsable del equipo	FECHA	HORA	TIPO			OBSERVACIONES
			A	B	C	

(A)RESPALDO COMPLETO: Respaldo de todos los ficheros y directorios
(B)RESPALDO DIFERENCIAL: Respaldo de todos los ficheros y directorios modificados desde el último respaldo completo
(C)RESPALDO INCREMENTAL: Respaldo de todos los ficheros y directorios modificados desde el último respaldo

Expedición: Acuerdo COTAIPEC/10/2021, sesión extraordinaria privada del 28/04/2021.

CÓDIGO DE ÉTICA Y REGLAS DE INTEGRIDAD DE LA COMISIÓN DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL ESTADO DE CAMPECHE

INTRODUCCIÓN.

El presente código contiene un conjunto de principios básicos de actuación y prácticas de conducta para todos los servidores públicos que trabajan en la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche.

Ningún servidor público puede ser obligado a cumplir órdenes o instrucciones contrarias a la ley, a la moral o a los principios contenidos en el presente Código. Si se presentara una situación de estas características, el servidor público deberá reportarla por escrito al Órgano Interno de Control, con el fin de que éste tome las medidas correspondientes.

Con fundamento en el artículo 16 de la Ley General de Responsabilidades Administrativas, el control de la aplicación y la divulgación del Código de Ética y las Reglas de Integridad de la Comisión es competencia del Órgano Interno de Control de la Comisión.

El presente documento define la dirección institucional a través de un conjunto de principios éticos que deberán ser cumplidos por todos los servidores públicos de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, en el desempeño de su empleo, cargo o comisión.

El Órgano Interno de Control de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche deberá informar al Pleno de ésta el diagnóstico y la evaluación de los resultados a que se refieren los artículos 15 y 17 de la Ley General de Responsabilidades Administrativas.

El lenguaje empleado en el Código de Ética no busca generar ninguna distinción ni marcar diferencias entre hombres y mujeres, por lo que las referencias o alusiones en la redacción representan y son dirigidas a ambos géneros.

Para los efectos del Código de Ética y de las reglas de Integridad se entenderá por:

a) **Código de Conducta**: El instrumento emitido por el Pleno de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche.
b) **Código de Ética**: El Código de Ética de los Servidores Públicos de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche a que se refiere el presente Acuerdo.
c) **Comité:** El Comité de Ética y de Prevención de Conflicto de Interés.

d) **Conflicto de Interés**: La situación que se presenta cuando los intereses personales, familiares o de negocios del servidor público puedan afectar el desempeño independiente e imparcial de sus empleos, cargos, comisiones o funciones.
e) **COTAIPEC:** Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche.
f) **Reglas de Integridad:** Las Reglas de Integridad para el ejercicio del servicio público, señaladas en el presente Acuerdo.
g) **Servidor público:** Persona que desempeña un empleo, cargo o comisión de cualquier naturaleza en la COTAIPEC.

CÓDIGO DE ÉTICA

Los Principios que todo servidor público de la COTAIPEC debe observar y conducir en el desempeño de su empleo, cargo, comisión o función, son los siguientes:

Disciplina. Evita comportamientos que generen dudas, afecten o atenten contra los valores e imagen de la Comisión.

Eficacia. Utilizar correctamente los recursos que le son asignados y cumplir con las obligaciones y funciones que le hayan sido atribuidas para el desempeño de su cargo exclusivamente para los fines a que están destinados.

Eficiencia. Actuando conforme a una cultura de servicio orientada al logro de resultados, procurando en todo momento un mejor desempeño de sus funciones a fin de alcanzar las metas institucionales según sus responsabilidades.

Honradez. Conduciéndose con rectitud sin utilizar su cargo para obtener o pretender la obtención de beneficio, provecho, ventaja personal o favor de terceros, ni buscar o aceptar compensaciones, prestaciones, dádivas, obsequios o regalos de cualquier persona u organización.

Integridad. Actuando siempre de manera congruente con los principios que deben observar en el ejercicio de un cargo, convencidos de ajustar su conducta para que en su desempeño impere una ética que responda al interés público y generen certeza plena de su conducta frente a las personas con las que se vinculen u observen su actuar.

Imparcialidad. Deberán dar a todas las personas el mismo trato por lo que no concederán privilegios o preferencia alguna, ni permitirán que influencias, intereses o perjuicios indebidos afecten su compromiso para tomar decisiones o ejercer sus funciones de manera objetiva.

Lealtad. Para corresponder a la confianza que la sociedad les confiere deberán mostrar vocación absoluta de servicio a la sociedad y preservar el interés superior de las necesidades colectivas por encima de intereses particulares, personales o ajenos al interés público y bienestar de la población.

Legalidad. Haciendo sólo aquello que expresamente les confieren las normas y en todo momento deben someter su actuación a las facultades que las leyes, reglamentos y demás disposiciones jurídicas atribuyen a su empleo, cargo o comisión por lo que conocen y cumplen con las disposiciones que regulan el ejercicio de sus funciones y atribuciones.

Objetividad. Para evitar prejuicios, conflictos de interés o influencia indebida de terceros que afecten el funcionamiento de la Comisión.

Profesionalismo. Para cumplir con el marco normativo para evitar cualquier acción que desacredite el ejercicio de sus funciones, facultades y atribuciones.

Rendición de cuentas. Asumiendo plenamente ante la sociedad y sus autoridades la responsabilidad que deriva del ejercicio de su cargo, por lo que informarán, explicarán y justificarán sus decisiones y acciones, sujetándose a un sistema de sanciones, a la evaluación y al escrutinio público de sus funciones por parte de la ciudadanía.

REGLAS DE INTEGRIDAD PARA EL EJERCICIO DE LA FUNCIÓN PÚBLICA EN LA COTAIPEC

Actuación pública.
El servidor público conducirá su actuación con transparencia, honestidad, lealtad, cooperación, austeridad, sin ostentación y con una clara orientación al interés público. Vulneran esta regla, de manera enunciativa y no limitativa, las conductas siguientes:

I. Abstenerse de ejercer las atribuciones y facultades que le imponen el servicio público y que le confieren los ordenamientos legales y normativos correspondientes;
II. Adquirir, para sí o para terceros, bienes o servicios de personas u organizaciones beneficiadas con programas o contratos gubernamentales a un precio notoriamente inferior o bajo condiciones de crédito favorables distintas a las del mercado;
III. Favorecer o ayudar a otras personas u organizaciones a cambio o bajo la promesa de recibir dinero, dádivas, obsequios, regalos beneficios personales o para terceros;
IV. Utilizar las atribuciones de su empleo, cargo, comisión o funciones para beneficio personal o de terceros;
V. Ignorar las recomendaciones de los organismos públicos protectores de los derechos humanos y de prevención de la discriminación u obstruir alguna investigación por violaciones en esas materias;

VI. Hacer proselitismo en su jornada laboral u orientar su desempeño laboral hacia preferencias político-electorales;
VII. Utilizar recursos humanos, materiales o financieros institucionales para fines distintos a los asignados;
VIII. Obstruir la presentación de denuncias administrativas, penales o políticas, por parte de compañeros de trabajo, subordinados o de ciudadanos en general;
IX. Asignar o delegar responsabilidades y funciones sin apegarse a las disposiciones normativas aplicables;
X. Permitir que servidores públicos subordinados incumplan total o parcialmente con su jornada u horario laboral;
XI. Realizar cualquier tipo de discriminación tanto a otros servidores públicos como a toda persona en general;
XII. Actuar como abogado o procurador en juicios de carácter penal, civil, fiscal, mercantil, administrativo, laboral o de cualquier índole que se promuevan en contra de la COTAIPEC;
XIII. Dejar de establecer medidas preventivas al momento de ser informado por escrito, como superior jerárquico, de una posible situación de riesgo o de conflicto de interés;
XIV. Hostigar, agredir, amedrentar, acosar, intimidar, extorsionar o amenazar al personal subordinado o compañeros de trabajo;
XV. Dejar de colaborar con otros servidores públicos y de propiciar el trabajo en equipo para alcanzar los objetivos comunes previstos en los planes y programas de la COTAIPEC;
XVI. Obstruir u obstaculizar la generación de soluciones a dificultades que se presenten para la consecución de las metas previstas en los planes y programas de la COTAIPEC;
XVII. Evitar conducirse bajo criterios de austeridad, sencillez y uso apropiado de los bienes y medios que disponga con motivo del ejercicio del cargo público, o
XVIII. Conducirse de forma ostentosa, incongruente y desproporcionada a la remuneración y apoyos que perciba con motivo de cargo público.

Información pública.

Los servidores públicos conducirán su actuación conforme al principio de transparencia y resguardarán la documentación e información que tienen bajo responsabilidad. Vulneran esta regla, de manera enunciativa y no limitativa, las conductas siguientes:

I. Asumir actitudes intimidatorias frente a las personas que requieren de orientación para presentar una solicitud de acceso a la información pública;
II. Retrasar de manera negligente las actividades que permitan atender de forma ágil y expedita las solicitudes de acceso a información pública;
III. Declarar la incompetencia para la atención de una solicitud de acceso a la información pública a pesar de contar con atribuciones o facultades legales o normativas;
IV. Declarar la inexistencia de información o documentación pública sin realizar una búsqueda exhaustiva en los expedientes y archivos institucionales bajo su resguardo;

V. Ocultar información y documentación pública en archivos personales, ya sea dentro o fuera de los espacios institucionales;
VI. Alterar, ocultar o eliminar, de manera deliberada, información pública;
VII. Permitir o facilitar la sustracción, destrucción o inutilización indebida, de información o documentación pública;
VIII. Proporcionar indebidamente documentación e información confidencial o reservada;
IX. Utilizar con fines lucrativos las bases de datos a las que tenga acceso o que haya obtenido con motivo de su empleo, cargo, comisión o funciones;
X. Obstaculizar las actividades para la identificación, generación, procesamiento, difusión y evaluación de la información en materia de transparencia proactiva y gobierno abierto;
XI. Difundir información pública en materia de transparencia proactiva y gobierno abierto en formatos que, de manera deliberada, no permitan su uso, reutilización o redistribución por cualquier interesado, o
XII. Cualquier otro tipo de conducta que sea contraria a las disposiciones contenidas en la legislación de la materia.

Contrataciones públicas, licencias, permisos, autorización y concesiones.
El servidor público que con motivo de su empleo, cargo, comisión o función, o a través de subordinados, participa en la celebración, otorgamiento o prórroga de dichas figuras, se conducirá con transparencia, imparcialidad y legalidad, orientando sus decisiones a las necesidades e intereses de la sociedad y que garanticen las mejores condiciones para el Estado. Vulneran esta regla, de manera enunciativa y no limitativa, las conductas siguientes:

I. Omitir declarar, conforme a las disposiciones aplicables, los posibles conflictos de interés, negocios y transacciones comerciales que, de manera particular, haya tenido con personas u organizaciones;
II. No aplicar el principio de equidad de la competencia que debe prevalecer entre los participantes dentro de los procedimientos de contratación;
III. Formular requerimientos diferentes a los estrictamente necesarios para el cumplimiento del servicio público, provocando gastos excesivos e innecesarios;
IV. Establecer condiciones en las invitaciones o convocatorias que representen ventajas o den un trato diferenciado a los licitantes;
V. Favorecer a los licitantes teniendo por satisfechos los requisitos previstos en las invitaciones o convocatorias cuando no lo están, simulando el cumplimiento de éstos o coadyuvando a su cumplimiento extemporáneo;
VI. Beneficiar a los proveedores sobre el cumplimiento de los requisitos previstos en las solicitudes de cotización;
VII. Proporcionar, de manera indebida, información de los particulares que participen en los procedimientos de contrataciones públicas;
VIII. Ser parcial en la selección, designación, contratación y, en su caso, remoción o rescisión del contrato en los procedimientos de contratación;

IX. Influir en las decisiones de otros servidores públicos para que se beneficie a un participante en los procedimientos de contratación o para el otorgamiento de licencias, permisos, autorizaciones y concesiones;
X. No imponer sanciones a licitantes, proveedores y contratistas que infrinjan las disposiciones jurídicas aplicables;
XI. Enviar correos electrónicos a los licitantes, proveedores, contratistas o concesionarios a través de cuentas personales o distintas al correo institucional;
XII. Reunirse con licitantes, proveedores, contratistas y concesionarios fuera de los inmuebles oficiales, salvo para los actos correspondientes a la visita al sitio;
XIII. Solicitar requisitos sin sustento para el otorgamiento y prorroga de licencias, permisos, autorizaciones y concesiones;
XIV. Dar trato inequitativo o preferencial a cualquier persona u organización en la gestión que se realice para el otorgamiento y prorroga de licencias, permisos, autorizaciones y concesiones;
XV. Recibir o solicitar cualquier tipo de compensación, dádiva, obsequio o regalo en la gestión que se realice para el otorgamiento y prorroga de licencias, permisos, autorizaciones y concesiones;
XVI. Dejar de observar el protocolo de actuación en materia de contrataciones públicas y otorgamiento de licencias, permisos, autorizaciones, concesiones y sus prorrogas, o
XVII. Ser beneficiario directo o a través de familiares de hasta cuarto grado, de contratos relacionados con la COTAIPEC.

Regla de integridad de programas gubernamentales.
Esta regla consiste en que los servidores públicos que, con motivo de su empleo, cargo o comisión, o a través de subordinados, participen en el otorgamiento y operación de subsidios y apoyos de programas gubernamentales, garantizando que la entrega de estos beneficios se apegue a los principios de igualdad y no discriminación, legalidad, imparcialidad, transparencia y respeto. Vulneran esta regla, de manera enunciativa y no limitativa, las conductas siguientes:

I. Ser beneficiario directo, o a través de familiares hasta el cuarto grado, de programas de subsidios o apoyos de la COTAIPEC;
II. Permitir la entrega o entregar subsidios o apoyos de programas gubernamentales de manera diferente a la establecida en las reglas;
III. Brindar apoyos o beneficios de programas gubernamentales a personas, agrupaciones o entes que no cumplan con los requisitos y criterios de elegibilidad establecidos en las reglas de operación;
IV. Difundir propaganda gubernamental con relación al otorgamiento de subsidios o apoyos de programas gubernamentales en periodos restringidos por la normatividad electoral, salvo en los casos en que ésta lo permita;

V. Dar trato inequitativo o preferencial a cualquier personal u organización en la gestión del subsidio o apoyo del programa, lo cual incluye el ocultamiento, retraso o entrega engañosa o privilegiada de información;
VI. Discriminar a cualquier interesado para acceder a los apoyos o beneficios de un programa gubernamental, o
VII. Alterar, disponer o hacer uso distinto a las atribuciones encomendadas de la información de los padrones de beneficiarios de programas gubernamentales diferentes a las atribuciones encomendadas.

Regla de integridad de trámites y servicios

Esta regla consiste en que los servidores públicos que, con motivo de su empleo, cargo, comisión o función, participen en la prestación de trámites o en el otorgamiento de servicios, atiendan a los usuarios de forma respetuosa, eficiente, oportuna, responsable e imparcial. Vulneran esta regla, de manera enunciativa y no limitativa, las conductas siguientes:

I. Ejercer una actitud contraria de servicio, respeto y cordialidad en el trato, incumpliendo protocolos de actuación o atención al público;
II. Otorgar información falsa sobre el proceso y requisitos para acceder a consultas, trámites, gestiones y servicios;
III. Realizar trámites y otorgar servicios de forma deficiente, retrasando los tiempos de respuesta, consultas, trámites, gestiones y servicios;
IV. Exigir, por cualquier medio, requisitos o condiciones adicionales a los señalados por las disposiciones jurídicas que regulan los trámites y servicios;
V. Discriminar por cualquier motivo en la atención de consultas, la realización de trámites y gestiones y la prestación de servicios, o
VI. Recibir, solicitar o aceptar, cualquier tipo de compensación, dádiva, obsequio o regalo en la gestión que se realice para el otorgamiento del trámite o servicio.

Regla de integridad de recursos humanos.

Esta regla consiste en que los servidores públicos que participen en procedimientos de recursos humanos, de planeación de estructuras o que desempeñen en general un empleo, cargo, comisión o función, se apeguen a los principios de igualdad y no discriminación, legalidad, imparcialidad, transparencia y rendición de cuentas. Vulneran esta regla, de manera enunciativa y no limitativa, las conductas siguientes:

I. Dejar de garantizar la igualdad de oportunidades en el acceso a la función pública con base en el mérito;
II. Designar, contratar o nombrar en un empleo, cargo, comisión o función a personas cuyos intereses particulares, laborales, profesionales, económicos o de negocios puedan estar en

contraposición o percibirse como contrarios a los intereses que les correspondería velar si se desempeñaran en el servicio público;

III. Proporcionar a un tercero no autorizado, información contenida en expedientes del personal y en archivos de recursos humanos bajo su resguardo;

IV. Suministrar información sobre los reactivos de los exámenes elaborados para la ocupación de plaza vacantes a personas ajenas a la organización de los concursos;

V. Seleccionar, contratar, nombrar o designar a personas sin haber obtenido previamente la constancia de no inhabilitación;

VI. Seleccionar, contratar, nombrar o designar a personas que no cuenten con el perfil del puesto, con los requisitos y documentos establecidos o que no cumplan con las obligaciones que las leyes imponen a todo ciudadano;

VII. Seleccionar, contratar, designar o nombrar directa o indirectamente como subalternos a familiares de hasta el cuarto grado de parentesco;

VIII. Inhibir la formulación o prestación de inconformidades o recursos que se prevean en las disposiciones aplicables para los procesos de ingreso;

IX. Otorgar a un servidor público subordinado, durante su proceso de evaluación, una calificación que no corresponda a sus conocimientos, actitudes, capacidades o desempeño;

X. Disponer del personal a su cargo en forma indebida, para que le realice tramites, asuntos o actividades de carácter personal o familiar ajenos al servicio público;

XI. Presentar información y documentación falsa o que induzca al error sobre el cumplimiento de metas de su evaluación del desempeño;

XII. Remover, cesar, despedir, separar o dar o solicitar la baja de servidores públicos de carrera sin tener atribuciones o por causas y procedimientos no previstos en las leyes aplicables;

XIII. Evitar que el proceso de evaluación del desempeño de los servidores públicos se realice en forma objetiva y, en su caso, dejar de retroalimentar sobre los resultados obtenidos cuando su desempeño sea contrario a lo esperado, o

XIV. Eludir, conforme a sus atribuciones, la reestructuración de áreas identificadas como sensibles o vulnerables a la corrupción o en las que se observe una alta incidencia de conductas contrarias al Código de Ética.

Regla de integridad de administración de bienes muebles e inmuebles

Esta regla consiste en que los servidores públicos que, con motivo de su empleo, cargo, comisión o función, participan en procedimientos de baja, enajenación, transferencia o destrucción de bienes muebles o de administración de bienes inmuebles, administren los recursos con eficiencia, transparencia y honradez para satisfacer los objetivos a los que están destinados. Vulneran esta regla de manera enunciativa y no limitativa, las conductas siguientes:

I. Solicitar la baja, enajenación, transferencia o destrucción de bienes cuando éstos sigan siendo útiles;

II. Compartir información con terceros ajenos a los procedimientos de baja, enajenación, transferencia o destrucción de bienes públicos, o sustituir documentos o alterar éstos;

III. Recibir o solicitar cualquier tipo de compensación, dádiva, obsequio o regalo a cambio de beneficiar a los participantes en los procedimientos de enajenación de bienes muebles e inmuebles;
IV. Intervenir o influir en las decisiones de otros servidores públicos para que se beneficie a algún participante en los procedimientos de enajenación de bienes muebles e inmuebles;
V. Tomar decisiones en los procedimientos de enajenación de bienes muebles e inmuebles, anteponiendo intereses particulares que dejen de asegurar las mejores condiciones en cuanto a precio disponible en el mercado;
VI. Manipular la información proporcionada por los particulares en los procedimientos de enajenación de bienes mubles e inmuebles;
VII. Utilizar cualquier tipo de vehículo propiedad o arrendado por la COTAIPEC para uso particular, personal o familiar, fuera de la normativa establecida por la propia Comisión;
VIII. Utilizar bienes inmuebles para uso ajeno a la normatividad aplicable, o
IX. Disponer de los bienes y demás recursos públicos sin observar las normas a las que se encuentran afectos y destinarlos a fines distintos al servicio público.

Regla de integridad de procesos de evaluación.
Esta regla consiste en que los servidores públicos que, con motivo de su empleo, cargo, comisión o función participen en procesos de evaluación, se apeguen en todo momento a los principios de legalidad, imparcialidad y rendición de cuentas. Vulneran esta regla, de manera enunciativa y no limitativa, las conductas siguientes:

I. Proporcionar indebidamente datos contenidos en los sistemas de información de la administración pública a la que tenga acceso con motivo de su empleo, cargo, comisión o función o acceder a tal información por causa distinta al ejercicio de sus funciones y facultades;
II. Transgredir el alcance y orientación de los resultados de las evaluaciones que realice cualquier instancia externa o interna en materia de evaluación o rendición de cuentas;
III. Dejar de atender las recomendaciones formuladas por cualquier instancia de evaluación, ya sea interna o externa, o
IV. Alterar registros de cualquier índole para simular o modificar los resultados de las funciones, programas y proyectos.

Regla de integridad de control interno.
Esta regla consiste en que los servidores públicos en el ejercicio de su empleo, cargo, comisión o función, que participen en procesos de control interno, generen, obtengan, utilicen y comuniquen información suficiente, oportuna, confiable y de calidad, apegándose a los principios de legalidad, imparcialidad y rendición de cuentas. Vulneran esta regla, de manera enunciativa y limitativa, las conductas siguientes:

I. Dejar de comunicar los riesgos asociados al cumplimiento de objetivos institucionales, así como los relacionados con corrupción y posibles irregularidades que afecten los recursos económicos públicos;
II. Omitir diseñar o actualizar las políticas o procedimientos necesarios en materia de control interno;
III. Generar información financiera, presupuestaria y de operación sin el respaldo suficiente;
IV. Comunicar información financiera, presupuestaria y de operación incompleta, confusa o dispersa;
V. Omitir supervisar los planes, programa o proyectos a su cargo o, en su caso, las actividades y el cumplimiento de las funciones del personal que le reporta;
VI. Dejar de salvaguardar documentos e información que se deban conservar por su relevancia o por sus aspectos técnicos, jurídicos, económicos o de seguridad;
VII. Ejecutar sus funciones sin establecer las medidas de control que le correspondan;
VIII. Omitir modificar procesos y tramos de control, conforme a sus atribuciones, en áreas en las que se detecten conductas contrarias al Código de Ética;
IX. Dejar de implementar o de adoptar mejores prácticas y procesos para evitar la corrupción y prevenir cualquier conflicto de interés;
X. Inhibir las manifestaciones o propuestas que tiendan a mejorar o superar deficiencias de operación, de procesos, de calidad de trámites y servicios o de comportamiento ético de los servicios públicos, o
XI. Eludir establecer estándares o protocolos de actuación en aquellos tramites y servicios con atención directa al público o dejar de observar aquellos previstos por las instancias competentes.

Regla de integridad de procedimiento administrativo

Esta regla consiste en que los servidores públicos que, en el ejercicio de su empleo, cargo, comisión o función participan en procedimientos administrativos, tengan una cultura de denuncia y respeten las formalidades esenciales del procedimiento y la garantía de audiencia conforme al principio de legalidad. Vulneran esta regla, de manera enunciativa y no limitativa, las conductas siguientes:

I. Omitir notificar el inicio del procedimiento y sus consecuencias;
II. Dejar de otorgar la oportunidad de ofrecer pruebas;
III. Prescindir el desahogo de pruebas en que se finque la defensa;
IV. Excluir la oportunidad de presentar alegatos;
V. Omitir señalar los medios de defensa que se pueden interponer para combatir la resolución dictada;
VI. Negarse a informar, declarar o testificar sobre hechos que le consten relacionados con conductas contrarias a la normatividad, así como al Código de Ética;
VII. Dejar de proporcionar o negar documentación o información que la autoridad competente requiera para el ejercicio de sus funciones o evitar colaborar con esta en sus actividades, o

VIII. Inobservar criterios de legalidad, imparcialidad, objetividad y discreción en los asuntos de los que tenga conocimientos que impliquen contravención a la normatividad, así como al Código de Ética o al Código de Conducta de la COTAIPEC.

Regla de desempeño permanente con integridad

Esta regla consiste en los servidores públicos que desempeñen un empleo, cargo, comisión o función, conduzcan su actuación con legalidad, imparcialidad, objetividad, transparencia, certeza, cooperación, ética o integridad. Vulneran esta regla, de manera enunciativa y no limitativa, las conductas siguientes:

I. Omitir conducirse con un trato digno y cordial, conforme a los protocolos de actuación o atención al público y de cooperación entre servidores públicos;
II. Retrasar, de manera negligente, las actividades que permitan atender de forma ágil y expedida al público en general;
III. Ocultar información y documentación con el fin de entorpecer las solicitudes de acceso a la información pública;
IV. Realizar actividades particulares en horarios de trabajo que contravengan las medidas aplicables para el uso eficiente, transparente y eficaz de los recursos públicos;
V. Aceptar documentación que no reúna los requisitos fiscales para la comprobación de gastos de presentación, viáticos, pasajes, alimentación, telefonía celular, entre otros;
VI. Obstruir la presentación de denuncias o acusaciones sobre el uso indebido o de derroche de recursos públicos, u
VII. Omitir excusarse de conocer asuntos que puedan implicar cualquier conflicto de interés.

Regla de cooperación con la integridad

Esta regla consiste en que los servidores públicos, en el desempeño de su empleo, cargo, comisión o función, cooperen con la COTAIPEC y con las instancias encargadas de velar por la observancia de los principios y valores intrínsecos a la función pública, en el fortalecimiento de la cultura ética y de servicio a la sociedad.

Son acciones que, de manera enunciativa y no limitativa, hacen posible propiciar un servicio público integro, las siguientes:

I. Detectar áreas sensibles o vulnerables a la corrupción;
II. Proponer o, en su caso, adoptar, cambios a las estructuras y procesos a fin de inhibir ineficiencias, corrupción y conductas no éticas, y
III. Recomendar, diseñar y establecer mejores prácticas a favor del servicio público.

Regla de integridad de comportamiento digno

Esta regla consiste en que los servidores públicos deben conducirse en forma digna sin proferir expresiones, adoptar comportamientos, usar lenguaje o realizar acciones de hostigamiento o acoso sexual, manteniendo para ello una actitud de respeto hacia las personas con las que tiene o guarda relaciones en la función pública. Vulneran esta regla, de manera enunciativa y no limitativa, las conductas siguientes:

I. Realizar a personas que sean compañeras de trabajo, personal subordinado o usuarios, señales sexuales sugerentes con las manos o a través de movimientos de otras partes del cuerpo;
II. Tener contacto físico sugestivo o de naturaleza sexual, con personas que sean compañeras de trabajo, personal subordinado o usuarios en horarios de trabajo;
III. Hacer regalos, dar preferencias indebidas o notoriamente diferentes en el ejercicio de su función, por tener interés sexual por una persona que sea compañera de trabajo, personal subordinado o usuario;
IV. Llevar a cabo conductas dominantes, agresivas, intimidatorias y hostiles durante horario laboral o hacia una persona que sea compañera de trabajo, personal subordinado o usuario, para que se someta a sus órdenes o intereses sexuales o al de otra u otras personas;
V. Espiar a una persona mientras se está en el sanitario;
VI. Condicionar la obtención de un empleo, su permanencia en él o las condiciones de éste a cambio de aceptar conductas de naturaleza sexual;
VII. Obligar a la realización de actividades que no competen a sus labores u otras medidas disciplinarias en represalia por rechazar proposiciones de carácter sexual;
VIII. Condicionar la prestación de un trámite o servicio público a cambio de que la persona usuaria o solicitante acceda a sostener conductas sexuales de cualquier naturaleza;
IX. Expresar palabras altisonantes, burlas, comentarios despectivos, hacia otra persona que sea compañera de trabajo, personal subordinado o usuario, referente a su apariencia;
X. Realizar comentarios, despectivos, burlas o broma sugerentes respecto de la vida sexual de una persona que sea compañera de trabajo, personal subordinado o usuario;
XI. Realizar invitaciones, favores o propuestas a citas o encuentros de carácter sexual directamente o mediante insinuaciones, a una persona que sea compañera de trabajo, personal subordinado o usuario;
XII. Emitir expresiones o utilizar lenguaje que denigre a las personas que sean compañeras de trabajo, personal subordinado o usuarios o pretenda colocarlas como objeto sexual;
XIII. Preguntar a una persona que sea compañera de trabajo, personal o subordinado o usuario sobre historias, fantasías, preferencias sexuales o su vida sexual;
XIV. Exhibir o enviar a través de algún medio de comunicación carteles, calendarios, mensajes, fotos, afiches, ilustraciones u objetos con imágenes o estructuras de naturaleza sexual, no deseadas ni solicitadas por la persona receptora, cuando ésta sea compañera de trabajo, personal subordinado o usuario;
XV. Difundir rumores o cualquier tipo de información sobre la vida de una persona que sea compañera de trabajo, personal subordinado o usuario;

XVI. Expresar insultos, lenguaje altisonante, gritos, malas palabras o humillaciones que afecten al respeto y la dignidad de las personas, o

XVII. Mostrar deliberadamente partes íntimas del cuerpo a una o varias personas que sean compañeras de trabajo, personal subordinado o usuario.

Comité de Ética y Prevención de Conflictos de Interés

La COTAIPEC contará con un Comité de Ética y de Prevención de Conflictos de Interés, que propicie la integridad de los servidores públicos e implemente acciones permanentes que favorezcan su comportamiento ético.

La integración y funcionamiento de dicho Comité deberá apegarse a lo dispuesto en la Ley General de Responsabilidades Administrativas y demás normatividad aplicable.

CÓDIGO DE ÉTICA Y REGLAS DE INTEGRIDAD APROBADOS MEDIANTE ACUERDO NÚMERO COTAIPEC/10/2021 POR EL PLENO DE LA COMISIÓN DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL ESTADO DE CAMPECHE EN LA SESIÓN EXTRAORDINARIA PÚBLICA CELEBRADA EL 28 DE ABRIL DE 2021.

LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE CAMPECHE Y SUS MUNICIPIOS

TÍTULO PRIMERO
DISPOSICIONES COMUNES PARA LOS ENTES PÚBLICOS

CAPÍTULO ÚNICO
DISPOSICIONES GENERALES

Artículo 1.- La presente Ley es de orden público e interés social y tiene por objeto proteger y garantizar los datos personales en poder de los Entes Públicos del Estado.

Artículo 2.- Esta Ley será aplicable a los datos personales que sean registrados en cualquier soporte físico, que permita su tratamiento por parte de las entidades del sector público.

Se exceptúan de su aplicación:

I. Los archivos que sean considerados como clasificados por la ley; y

II. Los archivos establecidos para investigaciones penales. En este caso, el responsable del archivo deberá comunicar la existencia del mismo a la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, indicando sus características generales y su finalidad.

Artículo 3.- Para los efectos de la presente Ley se entenderá por:

I. **Archivo:** El conjunto de datos de carácter personal, correspondientes a un grupo de personas, independientemente de su forma de creación, almacenamiento, tratamiento o uso;

II. **Archivo de acceso público:** El archivo que puede ser consultado por cualquier persona que no esté impedida por una disposición legal, ya sea gratuitamente o mediante el pago de los derechos correspondientes;

III. **Cesión de datos:** La comunicación o transmisión de datos hacia una persona distinta del interesado;

IV. **Comisión:** La Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, autoridad encargada de la aplicación del presente ordenamiento;

V. Consentimiento: La manifestación expresa, libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de datos personales de los que es titular;

VI. Datos personales: La información concerniente a una persona física identificada e identificable, relativa a su origen racial o étnico, o que este referida a sus características físicas, morales o emocionales, a su vida afectiva o familiar, domicilio, número telefónico, patrimonio, ideología, creencias o convicciones religiosas o filosóficas, su estado de salud físico o mental, sus preferencias sexuales, datos biométricos como la huella digital, datos sobre el DNA de las personas, claves informáticas o cibernéticas, códigos personales encriptados u otros análogos que se encuentren vinculados a su intimidad, entre otros.

VII. Encargado del tratamiento: El Ente Público que realice el tratamiento de datos por cuenta y con autorización del titular de los mismos;

VIII. Interesado o afectado: La persona física cuyos datos de carácter personal se incorporen al archivo o sistema;

IX. Ley: El presente ordenamiento;

X. Proceso de disociación: El tratamiento de los datos personales de modo que los datos resultantes no puedan ser relacionados directamente con ninguna persona identificable;

XI. Responsable del archivo o sistema: La persona física o moral, pública, encargada del tratamiento de los datos del archivo o sistema;

XII. Representante Legal: La persona autorizada por el titular de los datos para tener acceso a los mismos en su nombre y representación. La representación legal sólo se podrá acreditar mediante poder notarial.

XIII. Sistema de Datos Personales: Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los Entes Públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso;

XIV. Sujetos obligados: Los Entes Públicos a que se refiere la fracción IV del artículo 4 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.

XV. Tratamiento de datos: Las operaciones y procesos, automatizados o manuales, relacionados con la recolección, captura, conservación, proceso, transmisión, interrelación, combinación, control y otros manejos de los datos;

XVI. Unidad de Acceso: La unidad administrativa de los sujetos obligados receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales, a cuya tutela estará el trámite de las mismas, conforme a lo establecido en la presente Ley y en los lineamientos que expida la Comisión.

XVII. Usuario: Aquel autorizado por el Ente Público para prestarle servicios para el tratamiento de los sistemas de datos personales.

TÍTULO SEGUNDO
DE LA TUTELA DE LOS DATOS PERSONALES

CAPÍTULO I
DE LOS PRINCIPIOS

Artículo 4.- Los sistemas de datos personales en posesión de los Entes Públicos se regirán por los principios siguientes:

Licitud: Consiste en que la posesión y tratamiento de los sistemas de datos personales obedecerá exclusivamente a las atribuciones legales o reglamentarias de cada Ente Público y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Los sistemas de datos personales no pueden tener finalidades contrarias a las leyes o a la moral pública y en ningún caso pueden ser utilizados para finalidades distintas o incompatibles con aquella que motivaron su obtención. No se considerará incompatible el tratamiento posterior de los datos personales con fines históricos, estadísticos o científicos.

Consentimiento: Se refiere a la manifestación de la voluntad libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de sus datos personales.

Calidad de los Datos: Los datos personales recabados deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Los datos recabados deberán ser los que respondan con veracidad a la situación actual del interesado.

Confidencialidad: Consiste en garantizar que exclusivamente el titular o su representante legal pueden acceder a los datos personales o, en su caso, el responsable o el usuario del sistema de datos personales para su tratamiento, quienes deberán observar el deber de secrecía.

Los instrumentos jurídicos que correspondan a la contratación de servicios del responsable del sistema de datos personales, así como de los usuarios, deberán prever la obligación de garantizar la seguridad y la confidencialidad de los sistemas de datos personales, así como la prohibición de utilizarlos con propósitos distintos para los cuales se llevó a cabo la contratación, así como las penas convencionales por su incumplimiento. Lo anterior sin perjuicio de las responsabilidades previstas en otras disposiciones aplicables.

Los datos personales son irrenunciables, intransferibles e indelegables, por lo que no se podrán transmitir salvo disposición legal o cuando medie el consentimiento del titular y dicha obligación subsistirá aún después de finalizada la relación entre el Ente Público con el titular de los datos personales, así como después de finalizada la relación laboral entre el Ente Público y el responsable del sistema de datos personales o los usuarios.

El responsable del sistema de datos personales o los usuarios podrán ser relevados del deber de confidencialidad por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la seguridad nacional o la salud pública.

Seguridad: Consiste en garantizar que únicamente el responsable del sistema de datos personales o, en su caso, los usuarios autorizados puedan llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.

Disponibilidad: Los datos deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del interesado.

Temporalidad: Los datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubiesen sido recolectados.

Queda exceptuado el tratamiento que con posterioridad se les dé con objetivos estadísticos o científicos, siempre que cuenten con el procedimiento de disociación.

Únicamente podrán ser conservados de manera integra, permanente y sujetos a tratamiento los datos personales con fines históricos.

CAPÍTULO II
DE LOS SISTEMAS DE DATOS PERSONALES

Artículo 5.- Corresponde a cada Ente Público determinar, a través de su titular o, en su caso, del órgano competente, la creación, modificación o supresión de los sistemas de datos personales, conforme a su respectivo ámbito de competencia.

Artículo 6.- La integración, tratamiento y tutela de los sistemas de datos personales se regirán por las disposiciones siguientes:

I. Los archivos que contengan datos personales en posesión de los Entes Públicos deberán ser enlistados y dichas listas remitidas a la Comisión la cual deberá asegurarse que:

a) Los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida al momento de su recolección;

b) Ninguno de esos datos sea utilizado o revelado sin su consentimiento, con un propósito incompatible al que se haya especificado; y

c) El período de conservación de los datos personales sea el necesario para alcanzar la finalidad con que se hayan recolectado y registrado.

Cada Ente Público deberá publicar en su página de Internet la creación, modificación o supresión de sus sistemas de datos personales, dando aviso a la Comisión en los plazos y mediante los procedimientos establecidos en esta Ley y en los lineamientos que para tal efecto emita dicho organismo.

II. En caso de creación o modificación de los sistemas de datos personales, se deberá indicar por lo menos:

a) La finalidad del sistema de datos personales y los usos previstos para el mismo;

b) Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos;

c) El procedimiento de recolección de los datos de carácter personal;

d) La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo;

e) De la cesión de la que puedan ser objeto los datos;

f) Las instancias responsables del tratamiento del sistema de datos personales;

g) La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición; y

h) El nivel de protección exigible.

III. En las disposiciones que se dicten para la supresión de los sistemas de datos personales, se establecerá el destino de los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción.

IV. De la destrucción de los datos personales podrán ser excluidos aquellos que, con finalidades estadísticas o históricas, sean previamente sometidos al procedimiento de disociación.

Artículo 7.- Cuando los Entes Públicos recaben datos personales deberán informar previamente a los interesados de forma expresa, precisa e inequívoca lo siguiente:

I. De la existencia de un sistema de datos personales, del tratamiento de datos personales, la finalidad de la obtención de éstos y los destinatarios de la información;

II. Del carácter obligatorio o facultativo de responder a las preguntas que les sean planteadas;

III. De las consecuencias de la obtención de los datos personales, de la negativa asuministrarlos o de la inexactitud de los mismos;

IV. De la posibilidad para que estos datos sean difundidos, en cuyo caso deberá constar el consentimiento expreso del interesado, salvo cuando se trate de datos personales que por disposición de una ley sean considerados públicos;

V. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y

VI. Del nombre del responsable del sistema de datos personales y, en su caso, de los destinatarios.

Cuando se utilicen cuestionarios u otros impresos para la obtención de los datos, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el presente artículo.

En caso de que los datos de carácter personal no hayan sido obtenidos del interesado, éste deberá ser informado de manera expresa, precisa e inequívoca, por el responsable del sistema de datos personales, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad de lo previsto en las fracciones I, IV y V del presente artículo.

Se exceptúa de lo previsto en el presente artículo cuando alguna ley expresamente así lo estipule. Asimismo, tampoco regirá lo dispuesto en el presente artículo cuando los datos personales procedan de fuentes accesibles al público en general.

Artículo 8.- Ninguna persona está obligada a proporcionar datos personales considerados como sensibles, tal y como son: el origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencias sexuales.

Queda prohibida la creación de sistemas de datos personales que tengan la finalidad exclusiva de almacenar los datos señalados en el párrafo anterior y sólo pueden ser tratados cuando medien razones de interés general, cuando así lo disponga una ley, lo consienta expresamente el interesado o con fines estadísticos o históricos, siempre y cuando se hubiera realizado previamente el procedimiento de disociación.

Tratándose de estudios científicos o de salud pública, no será necesario el procedimiento de disociación.

Artículo 9.- Los archivos o sistemas creados con fines administrativos por los Entes Públicos, en los que se contengan datos de carácter personal, quedarán sujetos al régimen general de protección previsto en la presente Ley.

Los datos de carácter personal obtenidos para fines de seguridad pública, podrán ser recabados sin consentimiento de las personas a las que se refieren, pero estarán limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad, prevención o persecución de delitos, debiendo ser almacenados en sistemas específicos, establecidos para tal efecto, que deberán clasificarse por categorías en función de su grado de confiabilidad.

La obtención y tratamiento de los datos a los que se refiere el presente artículo, podrá realizarse exclusivamente en los supuestos en que sean absolutamente necesarios para los fines de una investigación concreta, sin perjuicio del control de legalidad en la actuación administrativa o de la obligación de resolver las pretensiones formuladas por los interesados ante los órganos jurisdiccionales.

Los datos personales recabados con estos fines se cancelarán cuando ya no sean necesarios para las investigaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del interesado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 10.- Los responsables de los sistemas de datos personales con fines de seguridad pública, para la prevención de conductas delictivas o en materia tributaria, podrán negar el acceso, rectificación, cancelación y oposición de los mismos, en función de los peligros que pudieran derivarse para la seguridad o la defensa del Estado, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, así como cuando los mismos obstaculicen la actuación de la autoridad durante el cumplimiento de sus atribuciones.

Artículo 11.- La cesión de los datos de carácter personal o su comunicación a terceros, se regirá por lo siguiente:

I. Toda cesión o comunicación a terceros deberá contar con el consentimiento expreso del interesado, excepto cuando:

a) La cesión haya sido autorizada en una ley;

b) Se trate de datos disponibles en fuentes de acceso público;

c) Sea necesario y esté previsto como parte de una relación jurídica;

d) Esté dirigida a las autoridades de seguridad pública o penales y cuente con autorización judicial;

e) Se trate de transferencias entre administraciones públicas;

f) Sea transferida para fines históricos, estadísticos o científicos; y

g) Se trate de datos sobre la salud y sean necesarios para atender una urgencia o para realizar estudios epidemiológicos;

II. El receptor de datos de carácter personal se obliga a acatar las disposiciones de la presente Ley;

III. Cuando la comunicación a terceros resulte de la prestación por parte de un tercero de servicios al responsable del archivo, el tercero en cuestión se considerará obligado en términos de la presente Ley, en las mismas condiciones que el responsable del archivo; y

IV. También queda obligado a acatar las disposiciones de la presente Ley, quien obtenga los datos en virtud de liquidación, fusión, escisión u otro cambio, en el caso de que los datos provengan de personas morales, o por herencia, en el caso de provenir de personas físicas.

CAPÍTULO III
DE LAS MEDIDAS DE SEGURIDAD

Artículo 12.- Los Entes Públicos establecerán las medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integralidad de cada sistema de datos personales que posean, con la finalidad de preservar el pleno ejercicio de los derechos tutelados en la presente Ley, frente a su alteración, pérdida, transmisión y acceso no autorizado, de conformidad con el tipo de datos contenidos en dichos sistemas.

Dichas medidas serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos personales; deberán constar por escrito y ser comunicadas a la Comisión para su registro.

Las medidas de seguridad que al efecto se establezcan deberán indicar el nombre y cargo del servidor público o, en su caso, la persona física o moral que intervenga en el tratamiento de los datos personales con el carácter de responsable del sistema o usuario, según corresponda. Cuando se trate de usuarios, se deberán incluir los datos del acto jurídico mediante el cual, el Ente Público otorgó el tratamiento del sistema de datos personales.

En el supuesto de actualización de estos datos, la modificación respectiva deberá notificarse a la Comisión dentro de los treinta días hábiles siguientes a la fecha en que se efectuó.

Artículo 13.- El Ente Público responsable de la tutela y tratamiento del sistema de datos personales, adoptará las medidas de seguridad, conforme a lo siguiente:

A. Tipos de seguridad:

I. **Física.-** Se refiere a toda medida orientada a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor;

II. **Lógica.-** Se refiere a las medidas de protección que permiten la identificación y autentificación de las personas o usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función;

III. **De desarrollo y aplicaciones.-** Corresponde a las autorizaciones con las que deberá contar la creación o tratamiento de sistemas de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas;

IV. **De cifrado.-** Consiste en la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la integralidad y confidencialidad de la información; y

V. **De comunicaciones y redes.-** Se refiere a las restricciones preventivas y/o de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a un dominio o cargar programas autorizados, así como para el manejo de telecomunicaciones.

B. Niveles de seguridad:

I. **Básico.-** Se entenderá como tal, el relativo a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas de datos personales. Dichas medidas corresponden a los siguientes aspectos:

a) Documento de seguridad;

b) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;

c) Registro de incidencias;

d) Identificación y autentificación;

e) Control de acceso;

f) Gestión de soportes, y

g) Copias de respaldo y recuperación.

II. **Medio.-** Se refiere a la adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo. Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los siguientes aspectos:

a) Responsable de seguridad;

b) Auditoria;

c) Control de acceso físico; y

d) Pruebas con datos reales.

III. **Alto.-** Corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos. Los sistemas de datos a los que corresponde adoptar el nivel de seguridad alto, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

a) Distribución de soportes;

b) Registro de acceso; y

c) Telecomunicaciones.

Los diferentes niveles de seguridad serán establecidos atendiendo a las características propias de la información.

Artículo 14.- Las medidas de seguridad a las que se refiere el artículo anterior constituyen mínimos exigibles, por lo que el Ente Público adoptará las medidas adicionales que estime necesarias para brindar mayores garantías en la protección y resguardo de los sistemas de datos personales. Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales y únicamente se comunicará a la Comisión, para su registro, el nivel de seguridad aplicable.

CAPÍTULO IV
DEL TRATAMIENTO DE DATOS PERSONALES

Artículo 15.- El tratamiento de los datos personales, requerirá del consentimiento inequívoco, expreso y por escrito del interesado, salvo en los casos y excepciones siguientes:

I. Cuando se recaben para el ejercicio de las atribuciones legales conferidas a los Entes Públicos;

II. Cuando exista una orden judicial;

III. Cuando se refieran a las partes de un convenio de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento;

IV. Cuando el interesado no esté en posibilidad de otorgar su consentimiento por motivos de salud y el tratamiento de sus datos resulte necesario para la prevención o para el diagnóstico médico, la prestación o gestión de asistencia sanitaria o tratamientos médicos, siempre que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente;

V. Cuando la transmisión se encuentre expresamente prevista en una ley;

VI. Cuando la transmisión se produzca entre organismos gubernamentales y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos;

VII. Cuando se den a conocer a terceros para la prestación de un servicio que responda al tratamiento de datos personales, mediante la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente que la comunicación de los datos será legítima en cuanto se limite a la finalidad que la justifique;

VIII. Cuando se trate de datos personales relativos a la salud y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos; y

IX. Cuando los datos figuren en registros públicos en general y su tratamiento sea necesario, con la condición de que no se vulneren los derechos y libertades fundamentales del interesado.

El consentimiento a que se refiere el presente artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

El Ente Público no podrá difundir o ceder los datos personales contenidos en los sistemas de datos desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento por escrito, o por un medio de autenticación similar, de las personas a que haga referencia la información. Al efecto, la oficina de información pública contará con los formatos necesarios para recabar dicho consentimiento.

El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente, debiendo responder solidariamente por la inobservancia de las mismas.

Artículo 16.- En los supuestos de utilización o cesión de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de derechos de las personas, la Comisión podrá requerir a los responsables de los sistemas de datos personales, la suspensión en la utilización o cesión de los datos. Si el requerimiento fuere desatendido, mediante resolución fundada y motivada, la Comisión podrá bloquear tales sistemas, de conformidad con el procedimiento que al efecto se establezca. El incumplimiento a la inmovilización ordenada por la Comisión será sancionado por la autoridad competente de conformidad con la Ley Reglamentaria del Capítulo XVII de la Constitución Política del Estado de Campeche.

Artículo 17.- El tratamiento de los sistemas de datos personales en materia de salud, se rige por lo dispuesto en la Ley General de Salud, la Ley de Salud para el Estado de Campeche y demás normas que de ellas deriven. El tratamiento y cesión de esta información obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico- asistencial, de manera tal que se mantenga la confidencialidad de los mismos, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación científica, de salud pública o con fines judiciales, en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales. El acceso a los datos y documentos relacionados con la salud de las personales queda limitado estrictamente a los fines específicos de cada caso.

Artículo 18.- Los sistemas de datos personales que hayan sido objeto de tratamiento, deberán ser suprimidos una vez que concluyan los plazos de conservación establecidos por las disposiciones aplicables, o cuando dejen de ser necesarios para los fines por los cuales fueron recabados.

En el caso de que el tratamiento de los sistemas haya sido realizado por una persona distinta al Ente Público, el instrumento jurídico que dio origen al mismo deberá establecer el plazo de conservación por el usuario, al término del cual los datos deberán ser devueltos en su totalidad al Ente Público, quien deberá garantizar su tutela o proceder, en su caso, a la supresión.

Artículo 19.- En caso de que los destinatarios de los datos sean instituciones de otras entidades federativas, los Entes Públicos deberán asegurarse que tales instituciones garanticen que cuentan con niveles de protección, semejantes o superiores, a los establecidos en esta Ley y en la propia normatividad del Ente Público de que se trate.

En el supuesto de que los destinatarios de los datos sean personas o instituciones de otros países, el responsable del sistema de datos personales deberá realizar la cesión de los mismos, conforme a las disposiciones previstas en la legislación federal aplicable, siempre y cuando se garanticen los niveles de seguridad y protección previstos en la presente Ley.

TÍTULO TERCERO
DEL EJERCICIO DE LOS DERECHOS EN MATERIA DE DATOS PERSONALES

CAPÍTULO I
DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN U OPOSICIÓN

Artículo 20.- Todas las personas, previa identificación mediante documento oficial, contarán con los derechos de acceso, rectificación, cancelación y oposición de sus datos personales en posesión de los Entes Públicos, siendo derechos independientes, de tal forma que el ejercicio de alguno de ellos no es requisito previo o impedimento para el ejercicio de otro.

La respuesta a cualquiera de los derechos previstos en la presente Ley deberá ser proporcionada en forma legible e inteligible, pudiendo suministrase, a opción del interesado, por escrito o mediante consulta directa.

Artículo 21.- El derecho de acceso se ejercerá para solicitar y obtener información de los datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las cesiones realizadas o que se prevén hacer, en términos de lo dispuesto por esta Ley.

Artículo 22.- Procederá el derecho de rectificación de datos del interesado, en los sistemas de datos personales, cuando tales datos resulten inexactos o incompletos, inadecuados o excesivos, siempre y cuando no resulte imposible o exija esfuerzos desproporcionados.

No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo o en un proceso judicial, aquellos se considerarán exactos siempre que coincidan con éstos.

Artículo 23.- El interesado tendrá derecho a solicitar la cancelación de sus datos cuando el tratamiento de los mismos no se ajuste a lo dispuesto en la Ley o en los lineamientos emitidos por la Comisión, o cuando hubiere ejercido el derecho de oposición y éste haya resultado procedente.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de los Entes Públicos para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el plazo, deberá procederse a su supresión, en términos de la normatividad aplicable.

La supresión de datos no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando exista una obligación legal de conservar dichos datos.

Artículo 24.- El interesado tendrá derecho a oponerse al tratamiento de los datos que le conciernan, en el supuesto en que los datos se hubiesen recabado sin su consentimiento, cuando existan motivos fundados para ello y la ley no disponga lo contrario. De actualizarse tal supuesto, el responsable del sistema de datos personales deberá cancelar los datos relativos al interesado.

Artículo 25.- Si los datos rectificados o cancelados hubieran sido transmitidos previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan transmitido, en el caso de que se mantenga el tratamiento por este último, quién deberá también proceder a la rectificación o cancelación de los mismos.

CAPÍTULO II
DEL PROCEDIMIENTO

Artículo 26.- La recepción y trámite de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales que se formulen a los Entes Públicos se sujetará al procedimiento establecido en el presente Capítulo y a los lineamientos que al efecto emita la Comisión.

Artículo 27.- Sin perjuicio de lo que dispongan otras leyes, sólo el interesado o su representante legal, previa acreditación de su identidad, podrán solicitar al Ente Público, a través de la Unidad de Acceso competente, que le permita el acceso, rectificación, cancelación o haga efectivo su derecho de oposición, respecto de los datos personales que le conciernan y que obren en un sistema en poder del sujeto obligado, mediante el cumplimiento de los siguientes requisitos:

I. Solicitud por escrito en la que se exprese el nombre, domicilio u otro medio para recibir notificaciones y los datos personales cuyo acceso, cancelación u oposición se requieren o la descripción clara de las correcciones a realizarse, acompañando los documentos que motiven su solicitud, en su caso;

II. Identificación oficial del solicitante;

III. Firma o huella digital; y

IV. Opcionalmente, la modalidad en la que prefiere se otorgue el acceso a sus datos personales, la cual podrá ser consulta directa, copias simples o certificadas. En ningún caso los datos personales solicitados o las correcciones realizadas podrán enviarse por medios electrónicos o entregarse en dispositivos magnéticos u ópticos.

Artículo 28.- La Unidad de Acceso correspondiente deberá notificar al solicitante en el domicilio o medio electrónico señalado para tales efectos, en un plazo máximo de veinte días hábiles contados a partir del día hábil siguiente a la presentación de la solicitud, la determinación adoptada en relación con su petición, a efecto de que, de resultar procedente, se haga efectiva la misma dentro de los diez días hábiles siguientes a la fecha de la citada notificación, previo pago de los derechos correspondientes, en su caso.

El plazo de veinte días hábiles referido en el párrafo anterior, podrá ser ampliado por una sola vez, por un período igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Artículo 29.- Cuando la solicitud resulte confusa, sea omisa en contener los detalles necesarios para la localización de los datos personales o no satisfaga alguno de los requisitos previstos en el presente Capítulo, la Unidad de Acceso procederá, dentro de los tres días siguientes a la recepción de la solicitud, a requerir al interesado para que, en el plazo de cinco días hábiles contados a partir del día siguiente del requerimiento, haga las aclaraciones pertinentes o subsane las omisiones en que haya incurrido. De no recibir la aclaración correspondiente, la solicitud se tendrá como no interpuesta.

Este requerimiento interrumpe el plazo establecido para dar respuesta a las solicitudes por parte de la Unidad de Acceso.

Artículo 30.- En el supuesto de que los datos personales a que se refiere la solicitud obren en los sistemas relativos del Ente Público, y éste considere improcedente la solicitud de acceso, rectificación, cancelación u oposición, se deberá emitir una resolución fundada y motivada al respecto. Dicha respuesta deberá estar firmada por el titular de la Unidad de Acceso y por el responsable del sistema de datos personales del Ente Público.

Cuando los datos personales respecto de los cuales se ejerciten los derechos de acceso, rectificación, cancelación u oposición, no sean localizados en los sistemas de datos del Ente Público, se hará del conocimiento del interesado a través de una resolución en la que se indiquen los sistemas de datos personales en los que se realizó la búsqueda. Dicha resolución deberá estar firmada por el titular de la Unidad de Acceso y por el responsable del sistema de datos personales del Ente Público.

Artículo 31.- Las solicitudes de acceso, rectificación, cancelación u oposición de datos personales, podrán ser presentadas por los medios siguientes, a elección del interesado o de su representante legal:

I. Personalmente, ante la Unidad de Acceso correspondiente, o bien, a través de correo ordinario, correo certificado o servicio de mensajería;

II. Por correo electrónico, a la dirección de correo electrónico asignada a la Unidad de Acceso del Ente Público; y

III. Por el sistema electrónico que la Comisión o el Ente Público establezcan para tal efecto.

Artículo 32.- En el caso de solicitudes de acceso a datos personales, el interesado o, en su caso, su representante legal, deberá acreditar su identidad y personalidad al momento de la entrega de la información. Asimismo, deberá acreditarse la identidad antes de que el Ente Público proceda a la rectificación o cancelación de los datos.

Artículo 33.- En el caso de solicitudes de rectificación de datos personales, el interesado deberá indicar el dato que es erróneo y la corrección que debe realizarse y acompañar la documentación probatoria que sustente su petición, salvo que la misma dependa exclusivamente del consentimiento del interesado y ésta sea procedente.

Artículo 34.- En el caso de solicitudes de cancelación de datos personales, el interesado deberá señalar las razones por las cuales considera que el tratamiento de los datos no se ajusta a lo dispuesto en la Ley o, en su caso, acreditar la procedencia del ejercicio de su derecho de oposición.

Artículo 35.- Los medios por los cuales el solicitante podrá recibir notificaciones serán: correo electrónico, sistema electrónico, notificación personal en su domicilio o en la Unidad de Acceso que corresponda. Si el interesado fuere omiso en señalar domicilio o dirección de correo electrónico, las notificaciones se le harán fijando una copia autorizada de la providencia o resolución en los estrados o cartelera de avisos de la Unidad de Acceso que corresponda.

El único medio por medio del cual el interesado o su representante legal podrán recibir la información referente a los datos personales será la Unidad de Acceso del Ente Público, sin mayor formalidad que la de acreditar su identidad y cubrir los costos de conformidad con la presente Ley y la legislación hacendaria del Estado; el titular también podrá recibir la información referente a sus datos personales por medio de correo certificado con notificación, previo pago de los derechos correspondientes.

El Instituto y los Entes Públicos contarán con la infraestructura y los medios tecnológicos necesarios para garantizar el efectivo acceso, rectificación, cancelación u oposición de los datos personales de los individuos con discapacidad.

Artículo 36.- La Comisión deberá expedir los lineamientos que establezcan de manera detallada los procedimientos a que se sujetará la recepción, procesamiento, resolución y notificación de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales.

Artículo 37.- El trámite de las solicitudes de acceso, rectificación, cancelación u oposición de datos de carácter personal es gratuito. No obstante, el interesado deberá cubrir los costos de reproducción de los datos solicitados, en términos de lo previsto por la legislación hacendaria del Estado.

Los costos de reproducción de la información solicitada se cobrarán al solicitante de manera previa a su entrega y se calculará atendiendo a:

I. El costo de los materiales utilizados en la reproducción de la información;

II. El costo de envío; y

III. La certificación de documentos cuando proceda.

Los Entes Públicos deberán esforzarse por reducir al máximo, los costos de entrega de la información.

CAPÍTULO III
DEL RECURSO DE REVISIÓN

Artículo 38.- Podrá interponer recurso de revisión ante la Comisión el interesado que se considere agraviado por la resolución que recaiga a su solicitud de acceso, rectificación, cancelación u oposición o ante la omisión de la respuesta. Para este efecto, las Unidades de Acceso al dar respuesta a las solicitudes, orientarán al particular sobre su derecho de interponer el recurso de revisión y el modo y plazo para hacerlo.

Artículo 39.- La Comisión tendrá acceso a la información contenida en los sistemas de datos personales que resulte indispensable para resolver el recurso. Dicha información deberá ser mantenida con carácter confidencial y no estará disponible en el expediente.

Las resoluciones que emita la Comisión podrán impugnarlas los particulares ante la Sala Administrativa del Tribunal Superior de Justicia del Estado, mediante el juicio de nulidad previsto en el Código de Procedimientos Contencioso-Administrativos del Estado; y las Unidades de Acceso ante el Pleno del citado Tribunal, conforme a las disposiciones establecidas en dicho Código para la tramitación del recurso de revisión. En este último caso la Comisión no podrá requerir la ejecución o cumplimento de su resolución hasta en tanto ésta no haya sido confirmada por el Tribunal Pleno.
La autoridad judicial competente tendrá acceso a los sistemas de datos personales cuando resulte indispensable para resolver el asunto y hubiera sido ofrecida en juicio. Dicha información deberá ser mantenida con ese carácter y no estará disponible en el expediente.

Artículo 40.- El recurso de revisión será tramitado de conformidad con los plazos, procedimientos y requisitos señalados en la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.

TÍTULO CUARTO
DE LA AUTORIDAD RESPONSABLE DEL CONTROL Y VIGILANCIA

CAPÍTULO ÚNICO
DE LA COMISIÓN

Artículo 41.- La Comisión será el organismo responsable de la tutela de los derechos consignados en la presente Ley.

Artículo 42.- La Comisión tendrá las atribuciones siguientes:

I. Vigilar el cumplimiento de esta Ley, particularmente en lo relativo a los derechos de datos personales;

II. Emitir los lineamientos para el ejercicio de los derechos en materia de acceso, rectificación, cancelación u oposición de datos personales, incluyendo los formatos correspondientes;

III. Conocer y resolver los recursos que se interpongan contra los actos y resoluciones emanados de los Entes Públicos, en los términos previstos en esta Ley y en la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche;

IV. Evaluar la actuación de los Entes Públicos en materia de protección de datos personales, mediante la práctica de visitas de inspección, emitiendo las recomendaciones o resoluciones a que hubiere lugar;

V. Informar a los ciudadanos acerca de sus derechos de acceso, rectificación, cancelación u oposición de datos de carácter personal y asesorarles en la materia;

VI. Elaborar y mantener actualizado el listado de los sistemas de datos personales en poder de los Entes Públicos, así como el registro de los niveles de seguridad establecidos por los mismos;

VII. Difundir y promover el ejercicio de los derechos plasmados en la presente Ley; y

VIII. Las demás que sean necesarias para el cumplimiento de las anteriores atribuciones.

Artículo 43.- En el Informe Anual que rinde la Comisión al H. Congreso del Estado, se deberá detallar la información concerniente a las solicitudes recibidas y tramitadas por los Entes Públicos en materia de acceso, rectificación, cancelación y oposición de datos personales, así como el estado de las impugnaciones recaídas a las mismas.

TÍTULO QUINTO
DE LAS RESPONSABILIDADES

CAPÍTULO ÚNICO
DE LAS INFRACCIONES Y SANCIONES

Artículo 44.- Son infracciones a la presente Ley:

I. No atender las solicitudes que presenten los interesados para el acceso, rectificación, cancelación u oposición de sus datos personales, cuando éstas procedan legalmente;

II. Recabar datos de carácter personal sin proporcionar la información especificada en la presente Ley;

III. No remitir a la Comisión los niveles de seguridad establecidos para la protección de los sistemas de datos personales en poder de los Entes Públicos;

IV. Obtener datos sin el consentimiento expreso del interesado cuando éste es requerido;

V. Incumplir los principios que rigen a los sistemas de datos personales, definidos en la presente Ley;

VI. Impedir, obstaculizar o negar el ejercicio de los derechos de los interesados en materia de datos personales establecidos en la presente Ley;

VII. La violación del secreto de los datos;

VIII. No remitir los listados de los sistemas de datos personales establecidas en la presente Ley a la Comisión, obstruir las funciones de la misma y no acatar sus disposiciones;

IX. La obtención de datos personales de manera engañosa o fraudulenta;

X. Tratar los datos de manera ilegítima; y

XI. La violación de la secrecía en el caso de los archivos de carácter policial, fiscal o de salud.

Artículo 45.- Las infracciones a que se refiere el artículo anterior o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en esta Ley, será sancionada en términos de la Ley Reglamentaria del Capítulo XVII de la Constitución Política de los Estados Unidos Mexicanos, siendo independientes de las de orden civil o penal que procedan, así como los procedimientos para el resarcimiento del daño ocasionado por el Ente Público.

Artículo 46.- La Comisión denunciará ante las autoridades competentes cualquier conducta prevista en el presente Capítulo y aportará las pruebas que considere pertinentes. Los órganos internos de control de los Entes Públicos entregarán semestralmente a la Comisión un informe estadístico de los procedimientos administrativos iniciados con motivo del incumplimiento de la presente Ley y sus resultados. Esta información será incorporada al Informe Anual de la Comisión.

T R A N S I T O R I O S

PRIMERO.- El presente decreto entrará en vigor a los quince días siguientes de su publicación en el Periódico Oficial del Estado.

SEGUNDO.- Los lineamientos para el acceso, rectificación, cancelación y oposición de los datos personales en poder de los entes públicos, serán actualizados o expedidos por la Comisión a más tardar dentro de los noventa días naturales siguientes a la entrada en vigor del presente decreto.

TERCERO.- Las solicitudes que antes de la entrada en vigor de la presente Ley, hayan presentado los particulares ante las Unidades de Acceso de los Entes Públicos, para que les proporcionen, modifiquen o cancelen sus datos personales que obren en archivo o sistema determinado, deberán concluir observándose las disposiciones contenidas en la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.

CUARTO.- Los entes públicos deberán notificar a la Comisión, sesenta días después de la entrada en vigor de la presente Ley, la relación de los Sistemas de Datos Personales que posean para su registro.

QUINTO.- El documento en el que se establezcan los niveles de seguridad a los que se refiere el Capítulo III del Título Segundo de la presente Ley, deberá ser emitido por los entes públicos dentro de los sesenta días posteriores a la entrada en vigor de la presente Ley, mismo que deberá ser remitido a la Comisión para su registro dentro del mismo plazo.

SEXTO.- Se derogan todas las disposiciones legales y reglamentarias en lo que se opongan al contenido del presente decreto.

Dado en el Salón de Sesiones del Palacio Legislativo, en la ciudad de San Francisco de Campeche, Campeche, a los diecinueve días del mes de junio del año dos mil doce.

C. Gloria del Carmen Gutiérrez Ocampo, Diputada Presidenta.- C. Silvia María Avilés Rivera, Diputada Secretaria.- C. José Benedicto Barony Blanquet, Diputado Secretario. Rúbricas.

En cumplimiento de lo dispuesto por los Artículos 48, 49 y 71 Fracción XVIII de la Constitución Política del Estado, lo sanciono, mando se imprima, publique y circule para su debida observancia.

Dado en el Palacio de Gobierno del Estado, en San Francisco de Campeche, Campeche, a los veinticinco días del mes de junio del año dos mil doce.- EL GOBERNADOR CONSTITUCIONAL DEL ESTADO, LIC. FERNANDO EUTIMIO ORTEGA BERNES.- LA SUBSECRETARIA "A" DE GOBIERNO, ENCARGADA DEL DESPACHO DE LA SECRETARÍA DE GOBIERNO, MTRA. PERLA KARINA CASTRO FARÍAS.- Rúbricas.

***NOTA**: El artículo segundo del decreto por el que se expide esta Ley establece lo siguiente: " Se deroga el Capítulo Séptimo "De la Protección de Datos Personales" del Título Primero "Disposiciones Comunes para los Sujetos Obligados", artículos del 31 al 38, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche, así como la fracción V del Artículo 3 del mismo ordenamiento jurídico."*

DECRETO NUM. 231 P.O. No. 5034 DE FECHA 09/JULIO/2012. LX LEGISLATURA.

Expedición: 06/11/2019, sesión COTAIPEC/CT/011/2019 del Comité de Transparencia de la COTAIPEC

Políticas Internas para la Protección de Datos Personales en Posesión de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche.

Objeto

El presente documento tiene por objeto establecer las políticas que deberán de seguir los servidores públicos de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche en la protección de los datos personales que traten con motivo de su empleo, cargo o comisión.

Marco Normativo

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el 4 de mayo de 2015.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.
- Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Campeche, publicada en el Periódico Oficial del Estado el 26 de julio de 2017.
- Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, publicados en el Periódico Oficial del Estado el 26 de enero de 2018.

Definiciones

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, fotográfica, acústica o 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. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética o biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales;

Responsable: La Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche;

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales relacionados con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales y, en general, cualquier otra actividad que involucre el uso o disposición de datos personales;

Unidad administrativa: Cada una de las áreas que conforman la estructura orgánica del responsable de conformidad con su reglamento interior.

Usuario: Cualquier persona que brinde sus servicios en la Comisión de Transparencia y Acceso a la Información del Estado de Campeche, que dé tratamiento o tenga acceso a los datos o a los sistemas de datos personales derivado de las funciones o atribuciones que le fueron conferidas con motivo del empleo, cargo, comisión o función que le haya sido asignado(a).

Prevención y Evaluación

Estas Políticas Internas constituyen un mecanismo preventivo en el tratamiento de datos personales, y su evaluación, al tratarse de medidas de seguridad de carácter administrativo, estará sujeta al mecanismo de monitoreo y revisión de las medidas de seguridad establecido en el “Documento de Seguridad de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche”, y estarán a sujetas a mejora continua.

POLÍTICAS INTERNAS PARA LA PROTECCIÓN DE DATOS PERSONALES.

1. El usuario deberá observar en todo momento las presentes políticas internas para la protección de datos personales, observando en el tratamiento de datos personales en todo momento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

2. Los datos personales sólo serán tratados por el o los usuarios autorizados para ello.

3. El usuario deberá en todo momento mantener el deber de confidencialidad de los datos personales que se encuentren bajo su custodia o a los que tenga acceso o conocimiento con motivo de su empleo, cargo, comisión o función y abstenerse de comunicarlos a quien no esté legalmente autorizado, tal deber subsistirá incluso después de finalizada la relación laboral con el responsable.

4. El usuario deberá resguardar en todo momento cualquier documento que contenga datos personales para evitar que terceros no autorizados tengan acceso a los mismos.

5. El usuario deberá de abstenerse de reutilizar hojas que contengan datos personales.

6. El usuario deberá abstenerse de reproducir, capturar o difundir mediante el uso de dispositivos de uso personal como celulares u otros cualquier documento que contenga datos personales.

7. El usuario deberá bloquear los equipos de cómputo bajo su resguardo cuando no se encuentren en uso y apagarlos al finalizar la jornada laboral.

8. El usuario deberá abstenerse de dejar a la vista en escritorios, impresoras, escáneres, fotocopiadoras, o en cualquier otro lugar documentos que contengan datos personales.

9. El usuario deberá procurar que los documentos que contengan datos personales, incluyendo aquellos considerados como sensibles, se encuentren resguardados en sitios bajo llave.

10. El usuario deberá procurar que las contraseñas utilizadas para el acceso a diversos sistemas que requiera para cumplimiento de sus funciones sean seguras, esto es,

mediante el uso o combinación de letras, mayúsculas, minúsculas, números y caracteres especiales.

11. El usuario deberá procurar que los documentos o dispositivos que contengan datos personales no sean extraídos del domicilio del responsable, para los casos en que ello resulte necesario por causas laborales, el usuario deberá implementar las medidas de seguridad necesarias para mantener la confidencialidad de los datos.

12. El usuario deberá cumplir en todo momento con las normas y procedimientos internos establecidos para el tratamiento de los datos personales.

13. El usuario deberá comunicar sin demora a su jefe inmediato cualquier vulneración de datos personales; en ausencia de éste tal comunicación deberá hacerse al superior jerárquico que siga en la cadena de mando, y se tomaran las medidas necesarias para aminorar el impacto producido por la vulneración.

14. El usuario deberá asegurarse de hacer saber al receptor de cualquier tipo de comunicación que involucre datos personales sobre la confidencialidad de la misma.

15. Sólo el personal autorizado de la Unidad Administrativa en cuestión podrá acceder a documentos que contengan datos personales bajo su custodia; para los casos en los que personal ajeno al de la unidad requiera tener acceso a documentos que contengan datos personales, deberá solicitarlo ante la unidad quién registrará el acceso en la bitácora establecida para ese efecto.

Estas Políticas fueron aprobadas por el Comité de Transparencia de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, en sesión ordinaria número COTAIPEC/CT/011/2019 celebrada el 6 de noviembre de 2019.

Transcripción para consulta, sin validez legal.
Verificar texto publicado en el Periódico Oficial del Estado (P.O.E.)

Expedición: Acuerdo COTAIPEC/006/2018, Sesión Extraordinaria Pública del Pleno de fecha 26/01/2018

LINEAMIENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE CAMPECHE

TÍTULO PRIMERO
DISPOSICIONES COMUNES PARA LOS SUJETOS OBLIGADOS

CAPÍTULO ÚNICO
DISPOSICIONES GENERALES

PRIMERO.- Los presentes lineamientos son de observancia obligatoria para los responsables a que se refiere la fracción XXX del artículo 3 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche y tienen por objeto garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de los sujetos obligados derivado del ejercicio de sus funciones, en términos de lo dispuesto por la Ley de referencia.

SEGUNDO.- Además de las definiciones contenidas en el artículo 3 de la Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Campeche, se entenderá por:

I. Acuse de recibo: documento con número de folio único que acredita la fecha de recepción de cualquier solicitud en la materia, independientemente del medio de recepción;

II. Finalidades: usos a los que el responsable van a destinar los datos personales recabados; responden a las preguntas ¿para qué van a ser recabados los datos personales? y ¿cuál es el destino que se le dará a ellos?;

III. Incidencia: cualquier acontecimiento que afecte o pudiera afectar la seguridad de los datos personales;

IV. Ley: Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Campeche, y

V. Lineamientos: Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche

TERCERO.- Categorías de datos personales.- Los datos personales contenidos en las bases de datos se clasificarán, de manera enunciativa, más no limitativa, de acuerdo a las siguientes categorías:

I. Datos de identidad: es toda aquella información que identifique o haga identificable a una persona como: el nombre, domicilio particular, teléfono particular, teléfono celular personal, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), número de matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, media filiación y demás análogos;

II. Datos electrónicos: es toda aquella información perteneciente a una persona física que sea utilizada para su identificación en Internet u otra red de comunicaciones electrónicas, como son: el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica o cualquier otra información empleada por la persona para su identificación;

III. Datos laborales: es toda aquella información que pertenezca a una persona, derivada de sus actividades y desarrollo profesional, por ejemplo: datos sobre su nombramiento, incidencia, capacitación o formación recibida, actividades extracurriculares, datos sobre la experiencia, desarrollo profesional, cargos o puestos desempeñados y demás análogos;

IV. Datos patrimoniales: es toda aquella información que pertenezca a una persona, referente a los bienes, derechos y obligaciones que conforman su patrimonio, por ejemplo: los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales crediticias o patrimoniales y demás análogos;

V. Datos sobre procedimientos administrativos o jurisdiccionales: la información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en cualquier rama del Derecho y demás análogos;

VI. Datos académicos: último grado de estudios, trayectoria académica, evaluaciones, calificaciones, títulos, cédula profesional, certificados o constancias escolares y demás análogos;

VII. Datos de tránsito y movimientos migratorios: información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria y demás análogos;

VIII. Datos sobre la salud: el expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de medicamentos, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona y demás análogos;

IX. Datos biométricos: es toda aquella información que se obtenga por medio de la aplicación de técnicas para la identificación de una persona a través de sus características fisiológicas y de comportamiento, como son: huellas dactilares, ADN, geometría de la mano, características de iris y retina y demás análogos;

X. Datos afectivos y/o familiares: es toda aquella información de una persona referente a sus sentimientos y emociones, así como la relativa a su entorno familiar, como son: estado civil, número de hijos, dependientes económicos, beneficiarios, referencias familiares y demás análogos, y

XI. Datos personales de naturaleza pública: aquellos que por mandato legal expreso sean accesibles al público, por ejemplo, nombre y percepciones de servidores públicos, nombre de beneficiarios de programas sociales y en general que reciban recursos públicos, cédula profesional, correo electrónico institucional, entre otros.

TÍTULO SEGUNDO
AVISO DE PRIVACIDAD

CAPÍTULO ÚNICO
DEL AVISO DE PRIVACIDAD

CUARTO.- Aviso de privacidad integral.- El domicilio del responsable.- El aviso de privacidad deberá señalar el domicilio del responsable.

El domicilio del responsable deberá indicar, al menos, la calle, número, colonia, ciudad, municipio o delegación, código postal y entidad federativa, y deberá corresponder a aquél para oír y recibir notificaciones.

TÍTULO TERCERO
INFORME ANUAL DE ACTIVIDADES

CAPÍTULO ÚNICO
DEL INFORME ANUAL DE ACTIVIDADES DE PROTECCIÓN DE DATOS PERSONALES

QUINTO.- Informe anual de solicitudes de ejercicio de derechos ARCO.- Los responsables, a través del Comité de Transparencia, deberán elaborar y presentar a la Comisión un informe anual de actividades realizadas en materia de protección de datos personales, a más tardar el último día hábil del mes de enero del año inmediato posterior al que corresponda dicho informe, en cumplimiento a lo establecido por el artículo 198 fracción XXIV de la Ley en correlación con el artículo 44 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

La Comisión emitirá el formato correspondiente y lo publicará en su página oficial en Internet, para conocimiento y uso por parte de los referidos responsables.

TÍTULO CUARTO
ACCIONES PREVENTIVAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO ÚNICO
DE LOS ESQUEMAS DE MEJORES PRÁCTICAS

SEXTO.- Validación o reconocimiento de los esquemas de mejores prácticas.- Los esquemas de mejores prácticas podrán incluir principios, normas y procedimientos para adecuar y armonizar las disposiciones en la Ley y abordar problemáticas o situaciones particulares que no fueron previstas por la norma general, a fin de hacer eficiente la protección de datos personales en las actividades que se autorregulen.

La adhesión a los esquemas de mejores prácticas por parte de un responsable o encargado es de carácter voluntario. No obstante, el cumplimiento de dichos esquemas será obligatorio para quienes se adhieran a los mismos, por lo que éstos deberán prever sanciones por su incumplimiento.

TÍTULO QUINTO
RECURSO DE REVISIÓN

CAPÍTULO ÚNICO
DE LA CONCILIACIÓN

SÉPTIMO.- Acta de la audiencia de conciliación.- De conformidad con lo señalado en la fracción II del artículo 144 de la Ley, de toda audiencia de conciliación se deberá levantar el acta respectiva. En dicha acta deberá constar, al menos, lo siguiente:

I. El número de expediente del recurso de revisión;

II. El lugar, fecha y hora de celebración de la audiencia de conciliación;

III. Los fundamentos legales para llevar a cabo la audiencia;

IV. El nombre completo del titular o su representante, ambos debidamente acreditados;

V. La denominación del responsable y su representante, este último debidamente acreditado;

VI. El nombre(s) de los servidores públicos de la Comisión que asistieron a la audiencia de conciliación;

VII. La manifestación de la voluntad del titular y del responsable de dirimir sus controversias mediante la celebración de un acuerdo de conciliación;

VIII. La narración circunstanciada de los hechos ocurridos durante la audiencia de conciliación;

IX. Los acuerdos adoptados por las partes, en su caso;

X. El plazo para cumplimiento de los acuerdos, en su caso, y

XI. El nombre y firma del conciliador designado por el Comisionado ponente, del titular o su representante, del representante del responsable y de todas aquellas personas que intervinieron en la audiencia de conciliación.

Cuando la audiencia de conciliación se realice por medios remotos o locales de comunicación electrónica, el conciliador deberá hacer del conocimiento de titular y responsable que la misma será grabada por el medio que a juicio del propio conciliador considere conveniente para el único efecto de acreditar la existencia de ésta.

OCTAVO.- Cumplimiento del acuerdo de conciliación.- El responsable deberá cumplir el acuerdo de conciliación en el plazo establecido en el acta, el cual se definirá en función del derecho ARCO a ejercer y de la complejidad técnica, operativa o demás cuestiones involucradas para hacer efectivo el derecho que se trate, la omisión de la respuesta correspondiente, o de portabilidad de datos.

Para tal efecto, el responsable deberá hacer del conocimiento del Comisionado ponente el cumplimiento del acuerdo a que se refiere el párrafo anterior del presente lineamiento a más tardar al día siguiente de que concluya el plazo fijado para cumplir el acuerdo de conciliación.

En caso de que el responsable no informe del cumplimiento dado al acuerdo de conciliación en el plazo establecido en el párrafo anterior, se tendrá por incumplido y se reanudará la sustanciación del recurso de revisión.

NOVENO.- Plazo para que el titular manifieste lo que a su derecho convenga respecto al cumplimiento del acuerdo de conciliación.- El Comisionado ponente deberá dar vista al titular para que manifieste lo que a su derecho convenga respecto al cumplimiento del acuerdo de conciliación remitido por el responsable, en un plazo máximo de tres días contados a partir del día siguiente de la recepción de notificación de cumplimiento del acuerdo de conciliación.

El titular tendrá un plazo máximo de tres días, contados a partir del día siguiente de la notificación a que se refiere el párrafo anterior del presente lineamiento, para que manifieste lo que a su derecho convenga. En caso de que el titular no esté de acuerdo con el cumplimiento del acuerdo de conciliación, deberá expresar sus motivos de inconformidad sin ampliar los agravios hechos valer a través del recurso de revisión.

Si el titular omite manifestarse, dentro del plazo señalado en el párrafo anterior, se entenderá su conformidad con el cumplimiento del acuerdo de conciliación a cargo del responsable.

DÉCIMO.- Efecto del cumplimiento del acuerdo de conciliación.- Cuando el responsable cumpla con el acuerdo de conciliación, el Comisionado ponente deberá emitir un acuerdo de cumplimiento, dentro de los tres días siguientes al plazo que se refiere el lineamiento anterior.

El cumplimiento del acuerdo de conciliación dará por concluida la sustanciación del recurso de revisión y el Comisionado ponente deberá someter a consideración del Pleno de la Comisión el proyecto de resolución en la que se proponga el sobreseimiento del recurso de revisión, en términos de lo dispuesto en la fracción V del artículo 153 de la Ley. En caso contrario, el Comisionado ponente deberá reanudar el procedimiento.

DÉCIMO PRIMERO.- Inconformidad del titular respecto al cumplimiento del acuerdo de conciliación.- Si el titular manifiesta su inconformidad respecto al cumplimiento del acuerdo de conciliación, la Comisión deberá analizar lo manifestado por el titular y el responsable, a efecto determinar si este último dio cumplimiento en los términos previstos en el acuerdo de conciliación.

De las manifestaciones realizadas por el titular y responsable, el Comisionado ponente podrá determinar:

I. El cumplimiento del acuerdo de conciliación y emitir el acuerdo a que se refiere el numeral anterior de los presentes Lineamientos, o

II. El incumplimiento del acuerdo de conciliación y emitir un acuerdo en el cual se reanude el procedimiento.

El Comisionado ponente deberá emitir el acuerdo a que se refieren las fracciones anteriores, dentro de los tres días siguientes contados a partir del día siguiente a la recepción de las manifestaciones del titular.

TRANSITORIOS

PRIMERO. Los presentes Lineamientos entrarán en vigor el mismo día de su aprobación por el Pleno de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche.

SEGUNDO.- El informe anual al que se refiere el lineamiento Quinto del presente cuerpo normativo, correspondiente al ejercicio 2017 deberá ser presentado a más tardar el día 15 de febrero de 2018.

ANEXOS
MODELOS DE AVISOS DE PRIVACIDAD

Anexo I: Modelo de Aviso de Privacidad simplificado

(Nombre de la Dirección/Unidad/Área a la que pertenece el aviso de privacidad)

Aviso de Privacidad simplificado de la base de datos personales
"(Nombre la base de datos personales)"

(Nombre del responsable), es el/la responsable del uso (tratamiento) y protección de los datos personales que nos proporcione, conforme a lo dispuesto por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche y demás normatividad aplicable.

Sus datos personales serán utilizados con las finalidades de: (señalar las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieran el consentimiento del titular).

En caso de que no desee que sus datos personales sean tratados para estas finalidades, usted puede manifestarlo (indicar mecanismos o medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales)

Se podrán transferir sus datos personales, en su caso, a (indicar a quién o quiénes), con la finalidad de dar (indicar las finalidades).

***En caso de que no realicen transferencias de datos personales**, podrá utilizar el siguiente texto: Se informa que no se llevarán a cabo transferencias de datos personales que requieran de su consentimiento expreso para poder efectuarlas, ya que conforme a la Ley de la materia sólo se realizarán aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.

Para mayor información acerca del tratamiento y de los derechos que puede hacer valer, usted puede acceder al aviso de privacidad integral a través de (el sitio o medio físico o electrónico donde se podrá acceder al aviso de privacidad integral).

Anexo II: Modelo de Aviso de Privacidad integral

(Nombre de la Dirección/Unidad/Área a la que pertenece el aviso de privacidad)

Aviso de Privacidad integral de la base de datos personales denominada "(Nombre la base de datos personales)"

(Nombre del responsable), con domicilio en (indicar domicilio del responsable), es la/el responsable del uso (tratamiento) y protección de los datos personales que nos proporcione, conforme a lo dispuesto por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche y demás normatividad aplicable.

Finalidades del tratamiento
Sus datos personales serán utilizados con las finalidades de: (señalar las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieran el consentimiento del titular).

En caso de que no desee que sus datos personales sean tratados para estas finalidades, usted puede manifestarlo (indicar mecanismos o medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales).

Datos personales recabados
Para las finalidades antes señaladas se recabarán los siguientes datos personales: (señalar los datos personales que serán sometidos a tratamiento, identificando aquéllos que sean sensibles, indicando cuáles son específicamente).

***Cuando no se recaben datos sensibles** se podrá utilizar el siguiente texto: Se informa que no se recabarán datos personales sensibles.

Fundamento legal para el tratamiento de datos personales
(Nombre del responsable) tratará los datos personales con fundamento en lo dispuesto en el artículo (indicar el fundamento legal que faculta expresamente al responsable para llevar a cabo el tratamiento de datos personales).

Transferencias de datos personales
Se podrán transferir sus datos personales, en su caso, a (indicar a quién o quiénes), con la finalidad de dar (indicar las finalidades).

***En caso de que no realicen transferencias de datos personales**, podrá utilizar el siguiente texto: Se informa que no se llevarán a cabo transferencias de datos personales que requieran de su consentimiento expreso para poder efectuarlas, ya que conforme a la Ley de la materia sólo se realizarán aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.

Derechos ARCO
Usted podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición de sus datos personales (derechos ARCO) directamente ante (señalar la dirección de la Unidad de Transparencia). O bien, a través de la Plataforma Nacional de Transparencia (http://www.plataformadetransparencia.org.mx/) o en el correo electrónico (correo electrónico de la unidad de transparencia). Si desea conocer el procedimiento para el ejercicio de estos derechos, puede acudir a la Unidad de Transparencia antes señalada o comunicarse al teléfono (número de teléfono de la Unidad de Transparencia).

Consulta del Aviso de Privacidad y cambios al mismo
Para mayor información acerca del tratamiento de sus datos personales y de los derechos que puede hacer valer, usted puede acceder al aviso de privacidad integral a través de (el sitio o medio físico o electrónico donde se podrá acceder al aviso de privacidad integral). En caso de realizar alguna modificación a este Aviso de Privacidad, el (nombre del responsable) le comunicará los cambios al aviso de privacidad a través del siguiente medio: (medio físico o electrónico a través del cual el responsable comunicará al titular tales cambios).

GUÍA PRÁCTICA PARA LA PROTECCIÓN DE *Datos Personales* EN EL ESTADO DE CAMPECHE

COTAIPEC

DIRECTORIO

1 *M.A.P. NÉSTOR CERVERA CÁMARA*
Comisonado Presidente

2 *M.A.P. TERESA DOLZ RAMOS*
Comisonada

3 *C.P. ROSA FRANCISCA SEGOVIA LINARES*
Comisonada

Comisión de Transparencia y Acceso a la Información Pública del Estado de Csampeche. (COTAIPEC).
Avenida Héroes de Nacozari No. 220, Col. Ampliación 4 Caminos, entre calle Tacubaya y Av. López Portillo, San Francisco de Campeche, Campeche, C.P. 24070

CONTENIDO

1 *PRESENTACIÓN*

2 *MARCO NORMATIVO*

3 *¿QUÉ SON LOS DATOS PERSONALES?*

4 *CATEGORÍAS DE DATOS PERSONALES*

5 *SUJETOS OBLIGADOS*

6 *PRINCIPIOS Y DEBERES EN PROTECCIÓN DE DATOS PERSONALES*

7 *DERECHOS ARCOP*

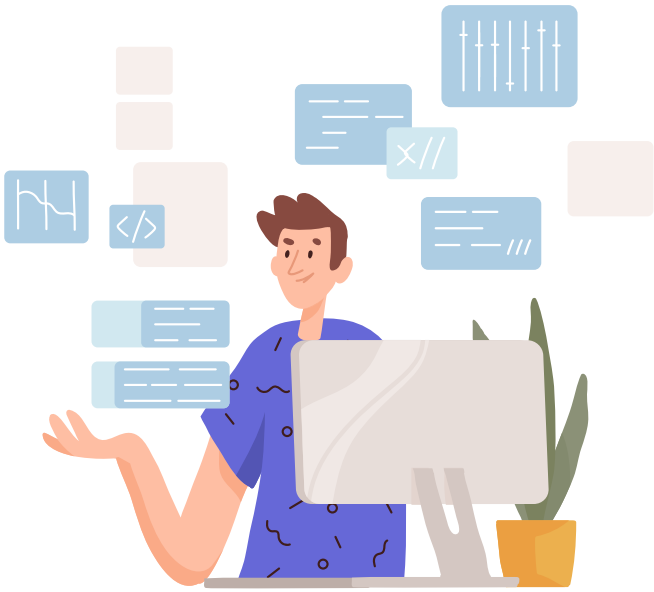
PRESENTACIÓN

La protección de datos personales se refiere al conjunto de medidas y prácticas que tienen como objetivo proteger la privacidad de las personas y garantizar que sus datos personales sean utilizados de manera responsable y ética.

Es además un derecho personalísimo, que únicamente puede ser ejercido por el titular de los datos personales, en su caso por su representante legal, debidamente acreditado para ello.

El derecho a la protección de datos personales regula el ejercicio de los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad al tratamiento de datos personales (Derechos ARCO). Además otorga a las personas físicas (titulares), la más amplia protección legal sobre sus datos personales, sometidos a cualquier tipo de tratamiento, ya sea por un sujeto de derecho público o privado.

Todo tratamiento o uso de datos personales puede conllevar un riesgo si se da un mal uso, una inadecuada gestión o cuidado, tener como consecuencia una intromisión ilegítima en la privacidad y la autodeterminación informativa de la persona que es titular de los datos personales. En ese sentido, al tratar datos personales se adquieren obligaciones para garantizar su adecuado tratamiento y decidir de manera libre e informada sobre el uso y destino de sus datos personales en posesión del responsable.

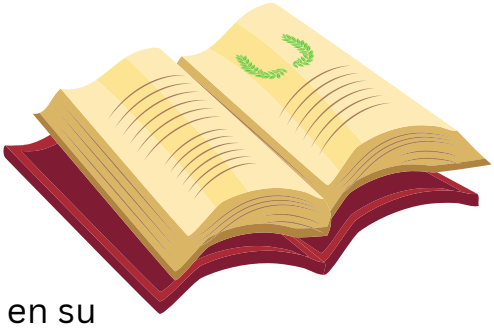


MARCO NORMATIVO

LAS NORMAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES ESTABLECEN LAS BASES, PRINCIPIOS Y PROCEDIMIENTOS PARA GARANTIZAR EL DERECHO QUE TIENEN TODA PERSONA A LA PROTECCIÓN DE SUS DATOS PERSONALES.

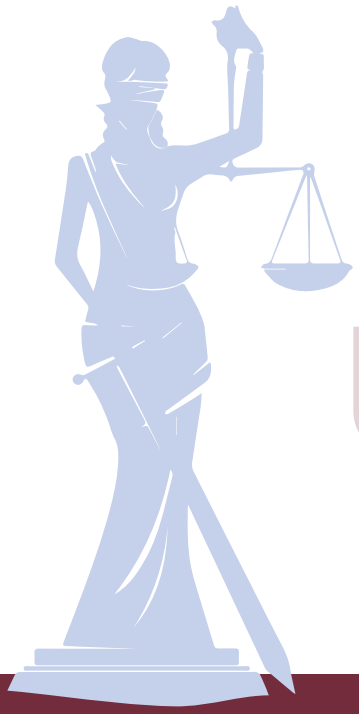
DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS

Adoptada y proclamada por la Asamblea General de las Naciones Unidas en París, en su resolución 217 A (III) (10 de diciembre de 1948).



ARTÍCULO 12

Nadie será objeto de injerencia arbitraria en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley.



CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

ARTÍCULO 6°

A.- Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

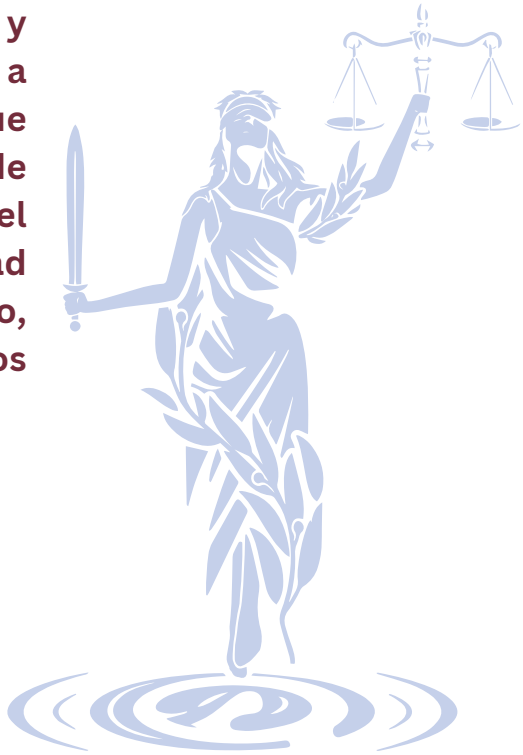
II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

ARTÍCULO 16°

Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.



LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

La **LGPDPPSO**, publicada en el Diario Oficial de la Federación el 26 de enero de 2017, tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados.

Son sujetos obligados (responsables) por esa Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE CAMPECHE

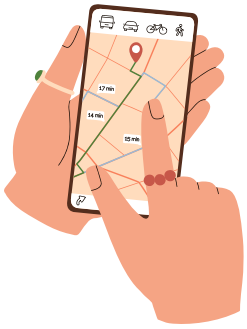
La presente Ley es de orden público y observancia general en todo el territorio del Estado de Campeche, y tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de los sujetos obligados.

¿QUÉ SON LOS DATOS PERSONALES?

Es cualquier información concerniente a una persona física identificada o identificable, de manera enunciativa más no limitativa.

Ejemplos de datos personales:

DOMICILIO



SEXO

ESTADO CIVIL

CARACTERÍSTICAS FÍSICAS

NÚMERO DE TELEFONO

DATOS PATRIMONIALES

Una persona es identificable cuando su identidad puede determinarse mediante los datos personales de que se traten.

¿QUÉ SON LOS DATOS PERSONALES SENSIBLES?

Son aquellos datos personales que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conllevar un riesgo grave para éste. Entre los datos personales sensibles encontramos los siguientes: origen racial o étnico; estado de salud (presente y futuro); información genética; creencias religiosas, filosóficas y morales; opiniones políticas y preferencia sexual.

CATEGORÍAS DE DATOS

IDENTIDAD

Es toda aquella información que identifique o haga identificable a una persona

- NOMBRE
- DOMICILIO PARTICULAR
- TELÉFONO PARTICULAR
- FIRMA
- CURP
- LUGAR Y FECHA DE NACIMIENTO, NACIONALIDAD
- EDAD

ELECTRÓNICOS

Es toda aquella información perteneciente a una persona física que sea utilizada para su identificación en Internet u otra red de comunicaciones electrónicas

- CORREO ELECTRÓNICO NO OFICIAL
- NOMBRE DE USUARIO
- CONTRASEÑAS
- FIRMA ELECTRÓNICA

LABORALES

Es toda aquella información que pertenezca a una persona, derivada de sus actividades y desarrollo profesional.

- DATOS SOBRE SU NOMBRAMIENTO
- INCIDENCIA
- CAPACITACIÓN O FORMACIÓN RECIBIDA
- DESARROLLO PROFESIONAL
- CARGOS O PUESTOS DESEMPEÑADOS Y DEMÁS ANÁLOGOS

PATRIMONIALES

Es toda aquella información que pertenezca a una persona, referente a los bienes, derechos y obligaciones que conforman su patrimonio

- BIENES MUEBLES E INMUEBLES
- INFORMACIÓN FISCAL
- HISTORIAL CREDITICIO, INGRESOS Y EGRESOS

PROCEDIMIENTOS ADMINISTRATIVOS O JURISDICCIONALES

Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en cualquier rama del Derecho y demás análogos.

ACADÉMICOS

- ÚLTIMO GRADO DE ESTUDIOS
- TRAYECTORIA ACADÉMICA
- EVALUACIONES
- CALIFICACIONES
- TÍTULOS
- CÉDULA PROFESIONAL
- CERTIFICADOS O CONSTANCIAS ESCOLARES Y DEMÁS ANÁLOGOS

TRÁNSITO Y MOVIMIENTOS MIGRATORIOS

Información relativa al tránsito de las personas dentro y fuera del país.

- **INFORMACIÓN MIGRATORIA Y DEMÁS ANÁLOGOS.**

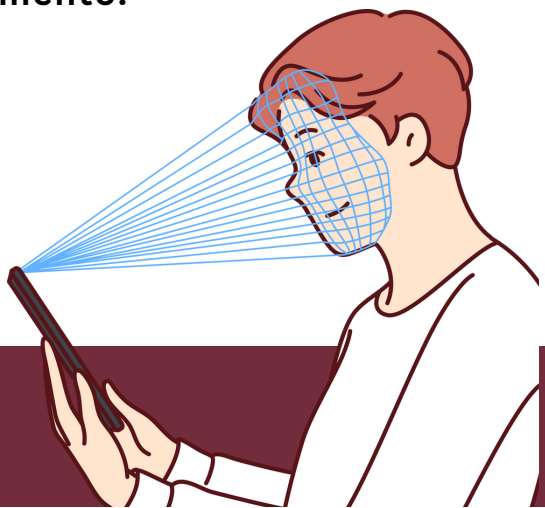
SALUD

- **EXPEDIENTE CLÍNICO DE CUALQUIER ATENCIÓN MÉDICA**
- **REFERENCIAS O DESCRIPCIÓN DE**
- **SINTOMATOLOGÍAS**
- **DETECCIÓN DE ENFERMEDADES**
- **INCAPACIDADES MÉDICAS**
- **DISCAPACIDADES**
- **INTERVENCIONES QUIRÚRGICAS**
- **VACUNAS**
- **CONSUMO DE MEDICAMENTOS, O ESTUPEFACIENTES**
- **USO DE APARATOS OFTALMOLÓGICOS, ORTOPÉDICOS, AUDITIVOS, PRÓTESIS, ASÍ COMO EL ESTADO FÍSICO O MENTAL DE LA PERSONA Y DEMÁS ANÁLOGOS.**

BIOMÉTRICOS

Es toda aquella información que se obtenga por medio de la aplicación de técnicas para la identificación de una persona a través de sus características fisiológicas y de comportamiento.

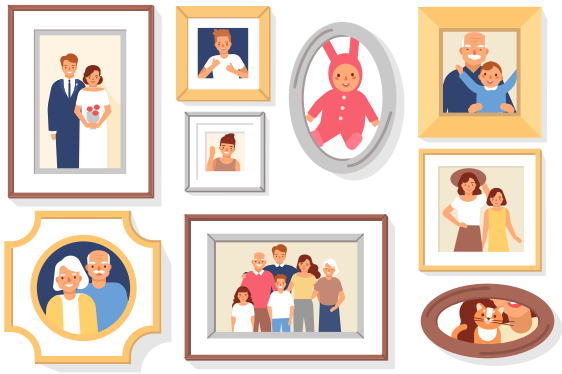
- **HUELLAS DACTILARES.**
- **ADN.**
- **GEOMETRÍA DE LA MANO.**
- **CARACTERÍSTICAS DE IRIS Y RETINA.**



NATURALEZA PÚBLICA
AFECTIVOS Y/O FAMILIARES

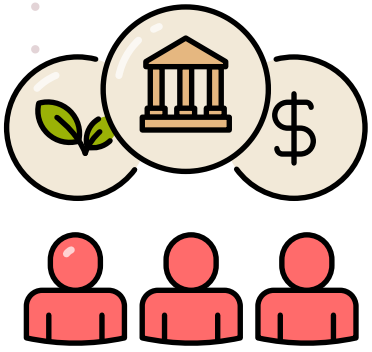
Es toda aquella información de una persona referente a sus sentimientos y emociones, así como la relativa a su entorno familiar.

- **ESTADO CIVIL.**
- **NÚMERO DE HIJOS.**
- **DEPENDIENTES ECONÓMICOS.**
- **BENEFICIARIOS.**
- **REFERENCIAS FAMILIARES.**



NATURALEZA PÚBLICA

Aquellos que por mandato legal expreso sean accesibles al público.



- **NOMBRE Y PERCEPCIONES DE SERVIDORES PÚBLICOS.**
- **NOMBRE DE BENEFICIARIOS DE PROGRAMAS SOCIALES Y EN GENERAL QUE RECIBAN RECURSOS PÚBLICOS.**
- **CÉDULA PROFESIONAL.**
- **CORREO ELECTRÓNICO INSTITUCIONAL**

¿QUIÉNES SON LOS SUJETOS OBLIGADOS?

Son sujetos obligados a cumplir con las disposiciones de la presente Ley, cualquier autoridad, dependencia, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Ayuntamientos, órganos, organismos autónomos, tribunales administrativos, fideicomisos y fondos públicos y partidos políticos del orden estatal y municipal del Estado de Campeche que lleven a cabo tratamientos de datos personales.

PRINCIPIOS Y DEBERES EN PROTECCIÓN DE DATOS PERSONALES

PRINCIPIOS

Los principios se traducen en obligaciones concretas para los responsables del tratamiento.

1. **LICITUD**

   Los responsables deben tratar los datos personales de manera lícita, conforme a lo dispuesto por la legislación mexicana y el derecho internacional aplicable, así como por la normativa que le resulte aplicable a cada responsable.

2. **CONSENTIMIENTO**

   Como regla general, el responsable debe obtener el consentimiento de la persona a quien pertenecen los datos personales, antes de utilizarlos.

3. **INFORMACIÓN**

   Obliga a los responsables a informar a los titulares, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

4. **CALIDAD**

   Radica en que los datos personales tratados deben ser exactos, completos, pertinentes, actualizados y correctos.

5. **FINALIDAD**

   Los datos personales únicamente podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad.

6. **LEALTAD**

   Establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

7. RESPONSABILIDAD

Consiste en la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales.

DEBERES

Además de los principios referidos con anterioridad, los responsables del sector público y privado deben de cumplir con los deberes de seguridad y confidencialidad, mismos que serán desarrollados a continuación.

1. DEBER DE SEGURIDAD

Es la obligación de establecer y mantener medidas de seguridad administrativas, físicas y técnicas con el propósito de proteger los datos personales contra daño, perdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

2. DEBER DE CONFIDENCIALIDAD

El deber de confidencialidad implica que el responsable debe guardar secreto respecto de los datos personales que son tratados, es decir, que los datos personales del titular no se difundan o compartan con terceros, salvo que se cuente con el consentimiento para ello, o bien, por alguna obligación normativa que exija su difusión.

DERECHOS ARCOP

EL ACRÓNIMO ARCOP ESTÁ CONFORMADO POR LAS INICIALES DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN Y PORTABILIDAD DE LOS DATOS PERSONALES, DERECHOS RECONOCIDOS POR LA LEGISLACIÓN MEXICANA Y QUE LOS TITULARES PUEDEN EJERCER, CONSISTEN EN:

A

ACCESO

Derecho que tiene el titular de solicitar el acceso a sus datos personales que se encuentran en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, y de conocer información relacionada con el tratamiento que se da a su información personal.

R

RECTIFICACIÓN

Es el derecho que tiene el titular de solicitar la rectificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados. Puede solicitar a quien posea o utilice sus datos personales que los corrija cuando los mismos sean incorrectos, desactualizados o inexactos.

C

CANCELACIÓN

Es el derecho que tienen los titulares de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los trata. No en todos los casos se podrán eliminar sus datos personales, principalmente cuando sean necesarios por alguna cuestión legal o el cumplimiento de obligaciones.

O

OPOSICIÓN

Es el derecho que tiene el titular de solicitar que sus datos personales no se utilicen para una determinada finalidad, no para la totalidad de estas. No siempre se podrá impedir el uso de los datos, cuento estos sean necesarios por motivos legales o para el cumplimiento de obligaciones.

P

PORTABILIDAD

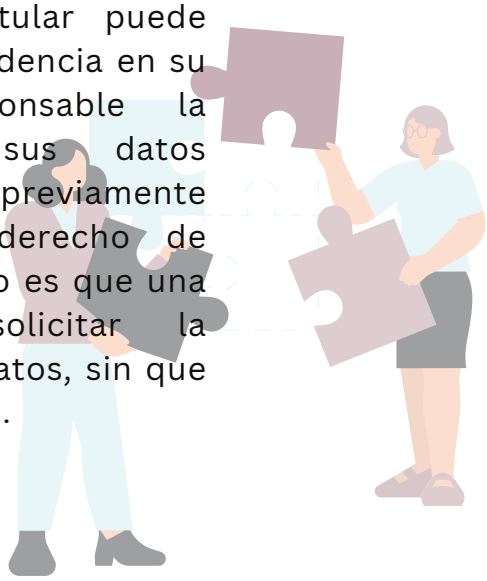
Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

¿CÓMO SE EJERCEN LOS DERECHOS ARCO?

El derecho a la protección de datos personales es un derecho personalísimo, solamente los titulares o sus representantes podrán solicitar el ejercicio de los derechos ARCO, por lo que es indispensable acreditar la identidad.

Para que un derecho sea ejercido no es necesario que lo haya sido previamente otro, ni el ejercicio de uno impide posteriormente el de uno distinto.

Por ejemplo, un titular puede solicitar a una dependencia en su carácter de responsable la rectificación de sus datos personales sin que previamente haya ejercido su derecho de acceso, otro supuesto es que una persona puede solicitar la cancelación de sus datos, sin que haya accedido a estos.



¿CUÁLES SON LOS REQUISITOS QUE DEBE TENER UNA SOLICITUD PARA EL EJERCICIO DE DERECHOS ARCO?

La solicitud debe presentar ante el responsable que posea los datos personales respecto de los cuales requieras el acceso, rectificación, cancelación u oposición.

Los requisitos que debe tener la solicitud son:

- El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;
- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;
- De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;

  IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;
- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y
- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

COTAIPEC

Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche

Si tienes alguna duda, sugerencia o queja

SOBRE COMO PUEDES EJERCER TU DERECHO A LA PROTECCIÓN DE DATOS PERSONALES,

ESCRIBE AL CORREO ELECTRÓNICO:
COTAIPEC@COTAIPEC.ORG.MX

O LLAMÁNOS:
9811271780 / 9818117953

LUNES A VIERNES DE 8:00 A 15:00 HORAS

EDICIÓN 2023
DIRECCIÓN DE PROTECCIÓN DE DATOS PERSONALES

AVISO DE PRIVACIDAD
INTEGRAL

Aviso de Privacidad integral de la base de datos personales **“Solicitudes de Ejercicio de Derechos ARCOP ”.**

La Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche (COTAIPEC), con domicilio en Av. Héroe de Nacozari, No. 220. Col. Ampliación Cuatro Caminos entre Tacubaya y Av. López Portillo, CP. 24070, San Francisco de Campeche, Campeche, es la responsable del uso (tratamiento) y protección de los datos personales que nos proporcione, conforme a lo dispuesto por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche y demás normatividad aplicable.

Finalidades del tratamiento.-Sus datos personales serán utilizados con las finalidades de dar atención a las solicitudes de ejercicio de derechos ARCO que se presenten ante la COTAIPEC, como responsable del tratamiento de los datos personales. En caso de que no desee que sus datos personales sean tratados para estas finalidades, usted puede manifestarlo presentando un escrito ante esta Comisión o a través del correo electrónico unidaddeacceso@cotaipec.org.mx.

Datos personales recabados.- Para la finalidad antes señalada se recabarán los siguientes datos personales: nombre completo del titular de los datos personales, nombre completo del representante legal, domicilio personal, correo electrónico personal e identificación oficial.

Se informa que no se recabarán datos personales sensibles.

AVISO DE PRIVACIDAD
INTEGRAL

Fundamento legal para el tratamiento de datos personales.- La COTAIPEC tratará los datos personales con fundamento en lo dispuesto en los artículos y 117 y 119 fracciones I y II de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

Transferencias de datos personales.- Se informa que no se llevarán a cabo transferencias de datos personales que requieran de su consentimiento expreso para poder efectuarlas, ya que conforme a la Ley de la materia sólo se realizarán aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.

Derechos ARCO.- Usted podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición de sus datos personales (derechos ARCO) directamente ante la Unidad de Transparencia de esta Comisión, o bien, a través de la Plataforma Nacional de Transparencia (http://www.plataformadetransparencia.org.mx/) o en el correo electrónico unidaddeacceso@cotaipec.org.mx Si desea conocer el procedimiento para el ejercicio de estos derechos, puede acudir a la Unidad de Transparencia antes señalada o comunicarse al teléfono de la COTAIPEC (981) 8117953 Ext. 103.

Consulta del aviso de privacidad y cambios al mismo.- Para mayor información acerca del tratamiento de sus datos personales y de los derechos que puede hacer valer, usted puede acceder a la versión digital de este aviso de privacidad integral a través de la página de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche COTAIPEC (http://www.cotaipec.org.mx/), o de manera presencial en las instalaciones de la Comisión. En caso de realizar alguna modificación a este Aviso de Privacidad, la COTAIPEC, le comunicará los cambios al aviso de privacidad a través de dicha página web.

AVISO DE PRIVACIDAD SIMPLIFICADO

Aviso de Privacidad simplificado de la base de datos personales **“Solicitudes de Ejercicio de Derechos ARCOP ”.**

La Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche (COTAIPEC), es la responsable del uso (tratamiento) y protección de los datos personales que nos proporcione, conforme a lo dispuesto por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche y demás normatividad aplicable.

Sus datos personales serán utilizados con las finalidades de dar atención a las solicitudes de ejercicio de derechos ARCO que se presenten ante la COTAIPEC, como responsable del tratamiento de los datos personales.

En caso de que no desee que sus datos personales sean tratados para estas finalidades, usted puede manifestarlo presentando un escrito ante esta Comisión o a través del correo electrónico unidaddeacceso@cotaipec.org.mx

Se informa que no se llevarán a cabo transferencias de datos personales que requieran de su consentimiento expreso para poder efectuarlas, ya que conforme a la Ley de la materia sólo se realizarán aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.

Para mayor información acerca del tratamiento de sus datos personales y de los derechos que puede hacer valer, usted puede acceder al aviso de privacidad integral a través de la página de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche COTAIPEC (http://www.cotaipec.org.mx/), o de manera presencial en las instalaciones de la Comisión.

TUS DATOS PERSONALES SON:

DOMICILIO

HISTORIAL CREDITICIO

NOMBRE Y FIRMA

CARACTERÍSTICAS FÍSICAS

NÚMERO DE TELEFONO

CORREO ELECTRÓNICO PERSONAL

Estos datos requieren de especial protección y cuidado, como cualquier otro bien importante para ti.

Para no ser utilizados con fines que pongan en riesgo o amenacen tu privacidad.

EXISTEN DATOS SENSIBLES

Hacen referencia a aspectos muy íntimos de tu vida.

EL ORIGEN RACIAL O ÉTNICO

CREENCIAS E IDEOLOGÍA

INFORMACIÓN GENÉTICA

ESTADO DE SALUD FÍSICO O MENTAL

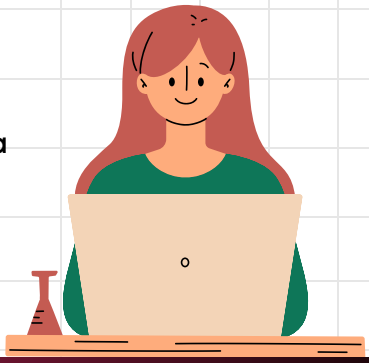
PREFERENCIA SEXUAL.

DERECHOS EN MATERIA DE DATOS PERSONALES

- **A** ACCESO
- **R** RECTIFICACIÓN
- **C** CANCELACIÓN
- **O** OPOSICIÓN
- **P** PORTABILIDAD

¿CÓMO EJERCER MIS DERECHOS?

Presentando una solicitud de Derechos ARCOP



¿CÓMO ACCEDO A MIS DATOS PERSONALES?

1. Personalmente: En la Unidad de Transparencia del Responsable.
2. Medios electrónicos.
3. A través de la Plataforma Nacional de Transparencia (PNT).

PROTECCIÓN DE DATOS PERSONALES

DERECHOS ARCOP

COTAIPEC

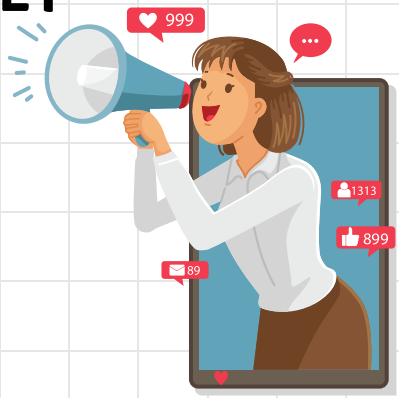
SEGURIDAD EN INTERNET

PROTECCIÓN DE DATOS PERSONALES

REDES SOCIALES

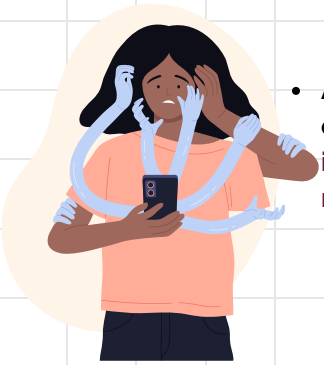
COTAIPEC

1 GENERA UN AMBIENTE SEGURO



- Mis redes sociales las mantengo **PRIVADAS**, elijo a quiénes acepto y con quiénes comparto mis publicaciones.
- Las conservo **SEGURAS**, **NO** uso las mismas contraseñas en mis cuentas, uso combinaciones de números y letras.

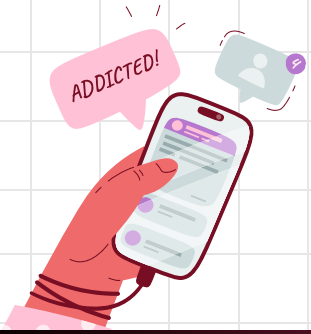
2 PIENSO ANTES DE PUBLICAR



- Antes de hacer un comentario o subir una fotografía, considero **¿Es realmente necesario publicarlo en internet?** ¿Obtendré algún beneficio? **¿Puede dañarme a mi o a otras personas?**

3 EMPATIZO SOCIALMENTE

- NO comparto fotos, videos o mensajes que ofendan a otros y me abstengo de tener un comportamiento negativo e hiriente. **TODO LO QUE HAGO EN INTERNET** puede perjudicar en la vida real.



4 CUIDO MI INTEGRIDAD

- **NO PROPORCIONO INFORMACIÓN** que ponga en riesgo mi seguridad, por ejemplo: Mi ubicación, mi rutina diaria, fotos de mis pertenencias, así como mi nombre completo, mi número de teléfono personal, mis claves, etc.

¿QUÉ ES EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES?

Es un derecho humano reconocido por el artículo 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos.

La Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche (COTAIPEC), garantiza la protección de tus datos personales.

¡SI TIENES ALGUNA DUDA!

PONEMOS A TU DISPOSICIÓN LOS SIGUIENTES CANALES:

9811271780 / 9818117953

datospersonales@cotaipec.org.mx

Lunes a Viernes de 8:00 a 15:00 hrs.
Avenida Héroes de Nacozari No. 220,
Col. Ampliación 4 Caminos, entre calle Tacubaya y Av. López Portillo,
San Francisco de Campeche, Campeche,
C.P. 24070

COTAIPEC

HABLEMOS DE :

PROTECCIÓN DE DATOS PERSONALES

¿QUÉ SON LOS DATOS PERSONALES?

Información que se relaciona con nuestra persona y nos identifica.

Nos dan identidad, nos describen y hacen diferentes a los demás.

EJEMPLOS

- DOMICILIO
- SEXO
- ESTADO CIVIL
- CARACTERÍSTICAS FÍSICAS
- NÚMERO DE TELEFONO
- DATOS PATRIMONIALES

DATOS SENSIBLES

Existen datos, que hacen referencia a aspectos muy sensibles.

- EL ORIGEN RACIAL O ÉTNICO
- CREENCIAS E IDEOLOGÍA
- INFORMACIÓN GENÉTICA
- ESTADO DE SALUD FÍSICO O MENTAL
- PREFERENCIA SEXUAL.

ESTOS DATOS REQUIEREN DE ESPECIAL PROTECCIÓN Y CUIDADO.

PROTEGE SIEMPRE TUS DATOS PERSONALES

Debes cuidarlos como cualquier otro bien importante para ti.

¿POR QUÉ?

Así tus datos no serán utilizados con fines que pongan en riesgo o amenacen tu privacidad.

¿EN DÓNDE HAY DATOS PERSONALES?

- BANCOS
- ESCUELAS
- HOTELES
- EMPRESAS
- REGISTRO CIVIL
- HOSPITALES

Esto debido a que realizamos trámites, compras o contratamos algún servicio.

LEY OLIMPIA

La **"Ley Olimpia"** implicó un conjunto de reformas a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal, a fin de reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas, a través de medios digitales. Contempla sanciones de 3 a 6 años de prisión para quienes realicen estas acciones y multas que van de 500 a 1,000 Unidades de Medida y Actualización (UMA).

¿SABÍAS QUÉ LA VIOLENCIA DIGITAL TAMBIÉN ES UN DELITO?

¡ALZA LA VOZ Y DENUNCIA!

¡SI TIENES ALGUNA DUDA!

PONEMOS A TU DISPOSICIÓN LOS SIGUIENTES CANALES:

9811271780 / 9818117953

datospersonales@cotaipec.org.mx

Lunes a Viernes de 8:00 a 15:00 hrs. Avenida Héroes de Nacozari No. 220,
Col. Ampliación 4 Caminos, entre calle Tacubaya y Av. López Portillo,
San Francisco de Campeche, Campeche,
C.P. 24070

COTAIPEC

PROTECCIÓN DE DATOS PERSONALES PARA LAS *Mujeres*

VIOLENCIA DIGITAL

¿QUÉ ES LA VIOLENCIA DIGITAL?

Es toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se expone, distribuye, difunde, exhibe, transmite, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona, sin su consentimiento, aprobación o autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.

EJEMPLOS DE VIOLENCIA DIGITAL

CIBERACOSO (CIBERBULLYING)

Uso de medios digitales, telefonía móvil y videojuegos online, principalmente, para acosar psicológicamente, amenazar, insultar, excluir o marginar a la víctima, al utilizar y difundir información confidencial o falsa.

ACOSO SEXUAL DIGITAL (GROOMING)

Cuando una persona intenta acercarse a ti, ganar tu confianza al fingir empatía, con el objetivo de obtener imágenes o videos, para satisfacer fines sexuales.

ESTAFA DIGITAL (PHISHING)

A través de mensajes de texto, llamadas, correos electrónicos o ventanas emergentes en internet, la ciber delincuencia busca conseguir información que revele contraseñas, datos de tarjetas de crédito o de la seguridad social y números de cuentas bancarias, entre otros, con el fin de cometer fraudes.

EXTORSIÓN SEXUAL (SEXTORSION)

Actos de chantaje que buscan obtener y/o exponer contenidos o material sexual como fotografías o videos, producidos por la víctima en situaciones previas de confianza y con base en amenazas. Es una forma de explotación sexual.

ATAQUE INFORMÁTICO (CRACKING)

Conducta delictiva de un individuo para alterar, modificar o eliminar el normal funcionamiento de un sistema informático, con la finalidad de acceder a cuentas bancarias, obtener imágenes o videos, entre otros

AUTOCUIDADO

Para protegerse de la Violencia Digital es necesario usar responsablemente las tecnologías de la información. Se requiere de una Alfabetización Digital que mejore la capacidad de comprender y aplicar la tecnología de manera positiva, para hacer que nuestra vida mejore o que seamos más productivos y eficientes. Te sugerimos:

1. Actualizar tus dispositivos para hacerlos menos vulnerables ante los ciberataques, como el uso de antivirus
2. Cifrar el contenido para que al acceder a cualquier información haya que introducir una clave de seguridad.
3. Gestionar contraseñas y patrones de desbloqueo seguros para que, además de no revelarlas a nadie, evites guardarlas en el dispositivo o utilizar una misma contraseña para todos los accesos. Usa una herramienta de gestión de claves.
4. Revisar tu dispositivo para detectar usos no controlados y verificar que no tengas aplicaciones que tú no hayas instalado.
5. Configurar tu privacidad en redes sociales. Revisa tus listas de amigos, apaga tu ubicación, cámara, micrófono y no compartas imágenes que pueden ponerte en riesgo.

COTAIPEC

SEGURIDAD EN INTERNET DE LOS DATOS PERSONALES

¿Cómo tener un comportamiento ON-LINE RESPONSABLE?

GENERO UN ENTORNO SEGURO

Mis redes sociales las mantengo PRIVADAS, eligiendo a quiénes acepto y con quiénes comparto mis publicaciones, las conservo SEGURAS, procuro no usar las mismas contraseñas en mis cuentas y uso combinaciones de números y letras.

PIENSO ANTES DE PUBLICAR

Antes de hacer un comentario o subir una fotografía, considero si es realmente necesario publicarlo en internet, si obtendré algún beneficio o si puede dañarme a mi o a otras personas.

EMPATIZO SOCIALMENTE

No contribuyo a generar daño a las personas, no comparto fotos, videos o mensajes que ofendan a otros y me abstengo de tener un comportamiento negativo ya que, todo lo que haga en internet puede perjudicar en la vida real.

CUIDO MI INTEGRIDAD

Tengo presente que en internet pudiera encontrarme un perfil falso, por eso no doy información que ponga en riesgo mi seguridad, por ejemplo: el domicilio en el que vivo, mis rutinas diarias, fotos de mis pertenencias, así como mi nombre completo, mi número de teléfono personal, mis claves, etc.

Cuando cuido mi PRIVACIDAD, PROTEJO mis Datos Personales.

#MISDERECHOSARCOP

COTAIPEC

Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche

¿SABÍAS QUÉ?

TUS **DATOS PERSONALES** SON: NOMBRE, FIRMA, CORREO ELECTRÓNICO NO OFICIAL, INCIDENCIAS LABORALES, HISTORIAL CREDITICIO, EXPEDIENTE CLÍNICO, HUELLAS DACTILARES, ESTADO CIVIL, ENTRE OTROS... Y GARANTIZAR SU PROTECCIÓN, CUANDO SE ENCUENTREN EN POSESIÓN DE SUJETOS OBLIGADOS ES UN **DERECHO HUMANO.**

¿POR QUÉ ES IMPORTANTE SU PROTECCIÓN?

PARA EVITAR QUE LOS DATOS SEAN UTILIZADOS CON UNA FINALIDAD DISTINTA A LA QUE FUERON PROPORCIONADOS, SEAN DIFUNDIDOS SIN AUTORIZACIÓN; GENERANDO INCLUSO ACTOS DE DISCRIMINACIÓN, SER VICTIMA DE UN DELITO, ENTRE OTROS SUPUESTOS.

¿CÓMO SE EJERCE ESA PROTECCIÓN?

COTAIPEC

ACCESO
RECTIFICACIÓN
CANCELACIÓN
OPOSICIÓN
PORTABILIDAD

PRESENTANDO UNA SOLICITUD

¿Cuándo?

¡En cualquier momento!

¿Dónde?

A través de estos medios legales:

- Unidad de Transparencia del Responsable
- Medios electrónicos
- Plataforma Nacional de Transparencia

Si tienes alguna duda sobre como ejercer tus derechos ARCOP, contáctanos en:

www.cotaipec.org.mx

cotaipec@cotaipec.org.mx

¡Síguenos!

@cotaipec

¿QUÉ SON LOS DATOS PERSONALES?

COTAIPEC

Información que se relaciona con nuestra persona y nos identifica.

DOMICILIO

SEXO

ESTADO CIVIL

CARACTERÍSTICAS FÍSICAS

NÚMERO DE TELEFONO

DATOS PATRIMONIALES

Nos dan identidad, nos describen y hacen diferentes a los demás.

DEBES CUIDARLOS COMO CUALQUIER OTRO BIEN IMPORTANTE PARA TI.

Lunes a Viernes de 8:00 a 15:00 hrs. Avenida Héroe de Nacozari No. 220, Col. Ampliación 4 Caminos, entre calle Tacubaya y Av. López Portillo, San Francisco de Campeche, Campeche, C.P. 24070

@COTAIPEC