



Deber de seguridad, medidas para la protección de los datos personales.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en su artículo 31, y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, en su artículo 49, contemplan el **deber de seguridad**. Ambas disposiciones obligan a los responsables a implementar y documentar una serie de medidas para garantizar la seguridad del tratamiento de los datos personales y protegerlos contra daño, pérdida, alteración, destrucción, o su uso, acceso a tratamiento no autorizado, estas medidas son de tres tipos: físicas, técnicas y administrativas.

En tal sentido, y con la finalidad de dar a conocer a los responsables la forma en la que deben dar cumplimiento a sus obligaciones derivadas del deber de seguridad, se elaboró la presente tabla en la que se proporcionan algunos ejemplos para cada uno de los tres tipos de medidas existentes y en la descripción se explica su forma de cumplimiento. En la tabla se documentan únicamente dos ejemplos de medidas de seguridad por cada tipo de medida, ello con la finalidad de demostrar de manera sencilla la forma en que debe darse su cumplimiento.

Sin perjuicio de lo anterior, los responsables, de manera individual, deberán implementar todas las medidas que resulten necesarias para garantizar la seguridad de los datos personales a los que den tratamiento, atendiendo a las particularidades propias de su institución, de los diversos tratamientos que realicen de conformidad con sus funciones y atribuciones, y de otros factores que pudieran incidir en la determinación de tales medidas como la capacidad económica del responsable.

Cabe señalar que, de las inquietudes expresadas por los responsables en diversos cursos de capacitación, se puede afirmar que la mayor parte de ellos implementan en la práctica algunas medidas de seguridad, sin embargo no las documentan como tal, y por tanto, no abonan al cumplimiento de sus obligaciones derivadas de la norma, en consecuencia, si se cuenta con tales medidas se debe proceder a su documentación, de lo contrario, a su implementación y documentación en la forma siguiente:



COMISIÓN DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL ESTADO DE CAMPECHE



Tipo de Medida	Medida	Finalidad	Descripción
Medidas de seguridad físicas	Instalación de cámaras de video vigilancia.	<ul style="list-style-type: none"> Prevenir el acceso no autorizado al perímetro de la organización. Prevenir el daño o interferencia a las instalaciones. 	Las instalaciones del responsable deben contar con cámaras de vigilancia ubicadas en sitios estratégicos como accesos y salidas de personas, o áreas o lugares críticos.
	Control de acceso a Unidades Administrativas	<ul style="list-style-type: none"> Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico. 	Las unidades administrativas del responsable deben contar con cerraduras en sus accesos físicos, las llaves o mecanismo de acceso deben estar bajo resguardo del titular de la unidad administrativa.
Medidas de seguridad técnicas	Software de seguridad	<ul style="list-style-type: none"> Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware. 	Los equipos de cómputo del responsable deben contar con software antivirus bajo licencia, para garantizar la seguridad de la información contenida en ellos.
	Mantenimiento de equipos	<ul style="list-style-type: none"> Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware. 	El responsable deberá realizar el mantenimiento preventivo de manera periódica de todos los equipos de cómputo y deberá llevar un registro de tales acciones mediante una bitácora.
Medidas de seguridad administrativas	Establecer políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales.	<ul style="list-style-type: none"> Delimitar las actuaciones en la gestión de los procedimientos internos. Establecer los principios que rigen el actuar de los servidores públicos del responsable 	El Comité de Transparencia deberá elaborar y aprobar una Política interna para la protección de datos personales, que será de observancia obligatoria para toda persona involucrada en el tratamiento de datos personales.
	Capacitación general y particular.	<ul style="list-style-type: none"> Sensibilizar y capacitar al personal en materia de protección de datos personales. Que el personal conozca y cumpla los principios, deberes, derechos y demás obligaciones, y las sanciones en caso de incumplimiento de las mismas. 	Todo personal involucrado en el tratamiento de datos personales deberá recibir capacitación general sobre la materia por lo menos una vez al año. Se recomienda que el personal de nuevo ingreso reciba capacitación dentro de los 90 días posteriores a su nombramiento. Dichas capacitaciones deberán constar en el programa general de capacitación de la institución.