CENACE®

CENTRO NACIONAL DE CONTROL DE ENERGÍA

CONTROLES DIRIGIDOS A ASEGURAR LA CONFIDENCIALIDAD QUE DEBEN GUARDAR TODAS LAS PERSONAS QUE INTERVIENEN EN CUALQUIER FASE DEL TRATAMIENTO DE DATOS PERSONALES.

OBJETIVO.

El presente documento tiene como finalidad dar cumplimiento a lo estipulado en los artículos 31 y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; así como del artículo 71 de los *Lineamientos Generales de Protección de Datos Personales para el Sector Público*, para proteger los datos personales, evitando, entre otras cosas, su divulgación no autorizada a terceros que pudiera poner en riesgo a sus titulares.

Lo anterior, es aplicable a todos los servidores públicos del Centro Nacional de Control de Energía que intervengan en cualquier fase del tratamiento de datos personales, quienes deberán guardar estricta confidencialidad de los mismos, para lo cual deben establecer los controles y mecanismos que garanticen el debido sigilo de los datos en cuestión, obligación que subsistirá aún después de finalizar su relación laboral.

De manera enunciativa más no limitativa, se sugiere seguir las siguientes pautas, ya que la difusión de información confidencial, ya sea por acción u omisión puede causar perjuicios a los titulares de los datos personales:

A. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, se deberán establecer y mantener medidas de seguridad de carácter administrativo[1], físico[2] y técnico[3] para la protección de éstos, que permitan protegerlos contra:

- Daño;

- [1] Protección de instalaciones, equipos, soportes o bases de datos personales.
- Utilización de candados, cerrojos, cerraduras, tarjetas de identificación, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de puertas, gavetas, cajones, archiveros, etc.
- Implementación de sistemas de vigilancia, alarmas, y de prevención y protección contra siniestros tales como incendios.
- Implementación de cámaras de seguridad.
- Resguardo de datos personales a través de infraestructura que garantice condiciones adecuadas de humedad, polvo, iluminación solar y temperatura y evite el deterioro por plagas, consumo de alimentos, y otros factores presentes en el entorno.

- [2] Identificación y autentificación de persona autorizada para el tratamiento de datos personales.
- Aprobación de normativa interna o políticas internas de tratamiento.
- Implementación de contraseñas, claves seguras y protocolos de seguridad.
- Identificación de roles y perfiles al interior del área que trata datos personales.
- Capacitación de personal.
- Elaboración de bitácoras de registro y seguimiento de las actividades que se realizan con la base de datos personales.
- Capacitación en materia de baja documental en soportes físicos y electrónicos.
- Emisión de reglas sobre la introducción de equipos de cómputo, accesorios y gadgets, o de conexión inalámbrica ajenas para el tratamiento de datos personales.

- [3] Encriptación y cifrado de los datos.
- Realización de copias de seguridad, resguardos o backups.
- Atención de fallas de equipo electrónico y de cómputo.
- Indicación de software autorizado.
- Des habilitación o cancelación de puertos de comunicación (USB, paralelo, serial, etc.); des habilitación o cancelación de dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.).
- Instalación de firewalls, antivirus, watchdogs, mecanismos para evitar la pérdida y filtración de datos (data loss prevention).

- Pérdida;
- Alteración;
- Destrucción, y
- Acceso o tratamiento no autorizado, como lo pueden ser: copia, distribución y reproducción.

B. En caso de elaborar un contrato, establecer cláusulas que obliguen a la confidencialidad de los datos personales a los terceros que intervengan en su tratamiento.

C. Elaborar al interior de las unidades administrativas - *acuerdos compromiso de confidencialidad* - que serán suscritos por los servidores públicos, con la finalidad de garantizar la debida protección de los datos personales.

D. Las personas que, con motivo de su empleo, cargo o comisión, tengan acceso a datos personales contenidos en medios electrónicos, deberán contar con contraseñas seguras las cuales no podrán ser compartidas con terceros.

E. Los datos personales contenidos en medios físicos deberán ser resguardados bajo llave, en espacios que garanticen su adecuada conservación.

F. Los papeles de oficina que contengan datos personales no podrán ser utilizados como papel de doble uso o de reciclado.

G. Se deberá informar con carácter inmediato al superior jerárquico, a la Jefatura de Unidad de Transparencia, así como al Órgano Interno de Control, sobre cualquier eventualidad relacionada con el uso indebido de datos personales de la que se tenga conocimiento en términos de los puntos anteriores, a efecto de que se tomen las acciones pertinentes y, en su caso, se emitan las sanciones que correspondan por parte de las Autoridades competentes.

H. Abstenerse de introducir a sus equipos de cómputo algún tipo de software, programa de cómputo, enlaces (links), virus o cualquier otro dispositivo que cause o sea susceptible de causar cualquier tipo de alteración o perjuicio.