Instituto de Transparencia
Acceso a la Información
Pública y Protección de Datos
Personales del Estado de Puebla

CATÁLOGO DE MEDIDAS DE SEGURIDAD QUE LOS SUJETOS OBLIGADOS PUEDEN CONSIDERAR PARA LA PROTECCIÓN Y SEGURIDAD DE LOS DATOS PERSONALES TRATADOS.

En términos de lo establecido por el artículo 46 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Por otro lado, de conformidad con el artículo 17 de los Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, en todo tratamiento de datos personales el responsable deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o acceso no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad administrativas, físicas y técnicas que el responsable podrá contemplar de manera enunciativa mas no limitativa son las siguientes:

a. **Medidas de seguridad administrativas**: 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 y protocolos de seguridad; identificación de roles y perfiles; realización de inventario de datos personales, análisis de riesgo y de brecha; elaboración de planes de trabajo para la futura implementación de medidas faltantes y necesarias; monitoreo y revisión periódica de las medidas; capacitación de personal; elaboración de bitácoras de registro y seguimiento de las actividades que se realizan con la base de datos personales; elaboración de procedimientos para dar aviso al personal custodio de los datos personales sobre la presencia y acceso de personas no autorizadas; emisión de reglas sobre la introducción de equipos de cómputo, accesorios y gadgets, o de conexión inalámbrica a áreas restringidas de tratamiento de datos personales; emisión de reglamentación interna que contemple infracciones y sanciones con relación al indebido tratamiento de datos personales; emisión de reglas para la baja documental en soportes físicos y electrónicos; emisión de medidas

para la prevención y notificación de intrusiones e incidentes; emisión de reglas de uso sobre dispositivos de almacenamiento externo; elaboración de manuales de operaciones; instauración de protocolos para casos de emergencia; realización de pruebas y simulacros; inclusión de cláusulas o contratos de confidencialidad para el personal laboral; procedimientos y canales para el ejercicio de derechos ARCO; procedimientos de disociación o pseudonimización; etc.

b. **Medidas de seguridad físicas**: 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; señalamiento de áreas de acceso restringido; aparatos de identificación por medio de la voz, iris, huella, ADN, y demás datos biométricos; 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; etc.

c. **Medidas de seguridad técnicas**: encriptación y cifrado de los datos; realización de copias de seguridad, resguardos o backups; almacenamiento en dos ubicaciones diferentes; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; deshabilitación o cancelación de puertos de comunicación (USB, paralelo, serial, etc.); deshabilitación o cancelación de dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.); deshabilitación o cancelación de dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etc,); realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; brindar soporte técnico de equipos, sistemas, programas de software, etc.; instalación de firewalls, antivirus, watchdogs, mecanismos para evitar la pérdida y filtración de datos (data loss prevention); segregación de funciones mediante perfiles de acceso; mecanismos de control de acceso; monitorización del uso de datos personales; implementación de técnicas de disociación o pseudonimización; etc.