**Medidas de seguridad previstas por la LGPDPPSO**

Los responsables deben adoptar medidas de seguridad que permitan proteger los datos personales contra daño, pérdida, alteración o destrucción; uso, acceso o tratamiento no autorizados; así como aquellas que garanticen la confidencialidad, integridad y disponibilidad de éstos.

Factores para determinar y establecer las medidas de seguridad de carácter:

• **Administrativas**

**• Físicas**

**• Técnicas**

**Las medidas de seguridad administrativas** se refieren al establecimiento de políticas y procedimientos para:

a) La gestión, soporte y revisión de la seguridad de la información a nivel organizacional.

b) La identificación, clasificación y borrado de la información.

**Las medidas de seguridad técnicas** se refieren al establecimiento de políticas y procedimientos para:

• Asegurar que el acceso a las bases de datos sea por usuarios identificados y autorizados.

• Generar privilegios o perfiles de acceso a los datos personales en función de las atribuciones y funciones de cada usuario.

• Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.

• Revisar la configuración de seguridad del software y hardware.

• Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

**Las medidas de seguridad físicas** se refieren al establecimiento de políticas y procedimientos para:

• Prevenir el acceso no autorizado al perímetro de la organización, instalaciones físicas, áreas críticas, recursos e información.

• Prevenir daño o interferencia a instalaciones físicas, áreas críticas de la organización, recursos e información.

• Proteger recursos móviles, portátiles, soportes físicos o electrónicos que salgan de la organización.

• Proveer a equipos que almacenan datos personales de mantenimiento eficaz.

* **Documento de Seguridad**

Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

• El inventario de datos personales y de los sistemas de tratamiento,

• Las funciones y obligaciones de las personas que traten datos personales,

• El análisis de riesgos.

• El análisis de brecha.

• El plan de trabajo.

• Los mecanismos de monitoreo y revisión de las medidas de seguridad.

• El programa general de capacitación.

* **Esquemas de mejores prácticas**

La Ley establece que el responsable puede adoptar—en lo individual o con el acuerdo de otros responsables, encargados u organizaciones—esquemas de mejores prácticas que tienen por objeto:

• Elevar el nivel de protección de los datos personales.

• Armonizar el tratamiento de datos personales en un sector específico.

• Facilitar el ejercicio de los derechos ARCO por parte de los titulares.

• Facilitar las transferencias de datos personales.

• Complementar las disposiciones previstas en la normatividad de datos personales.

• Demostrar ante el organismo garante el cumplimiento de esa normatividad.

El objetivo principal de los esquemas de mejores prácticas es optimizar la seguridad de los datos personales a partir de establecer un estándar de protección de datos personales mayor a las obligaciones previstas en la Ley General.