REGLAMENTO DEL PROGRAMA PROFESIONALIZANTE DE DELEGADOS DE PROTECCIÓN DE DATOS PERSONALES

La Superintendencia de Protección de Datos Personales, mediante resolución No. SPDP-SPD-2025-0004-R ha aprobado el Reglamento del Programa Profesionalizante de Delegados de Protección de Datos Personales, con el objetivo de garantizar que los profesionales encargados del tratamiento de datos personales actúen de forma proactiva y adecuada conforme con la Ley Orgánica de Protección de Datos Personales y los principios del ordenamiento jurídico vigente.

¿CUÁLES SON LOS PUNTOS IMPORTANTES?

PERFIL PROFESIONAL REQUERIDO

Los Delegados de Protección de Datos Personales deberán contar con cualificaciones en:

- Derecho
- Tecnologías de la información y comunicación
- Sistemas

RESPONSABILIDAD DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

- Son las únicas autorizadas para impartir programas académicos del Programa Profesionalizante.
- Deberán implementar el contenido del Anexo I en sus programas de tercer, cuarto nivel y educación continua.
- Están obligadas a notificar a la Superintendencia (SPDP) sobre los títulos, certificados o diplomas expedidos, para su registro en la plataforma correspondiente.

IMPLEMENTACIÓN DEL PROGRAMA

- Las instituciones que ya ofrezcan formación en esta área tienen un plazo de seis meses desde la publicación de la resolución en el Registro Oficial para adaptarse al nuevo Programa.
- En el mismo plazo, la SPDP deberá implementar la plataforma de registro académico.

ESTRUCTURA ACADÉMICA DEL PROGRAMA (ANEXO I)

El programa contempla un mínimo de 80 horas y se divide en los siguientes bloques:

- **Derecho de Protección de Datos Personales**
  Incluye: naturaleza jurídica, principios, derechos del titular, bases de legitimación, transferencias internacionales de datos personales, obligaciones ante la SPDP, régimen sancionador y fenómenos culturales, tecnológicos y económicos que afectan la privacidad.
- **Metodológico**
  Desarrolla la implementación de un Sistema de Gestión de Protección de Datos, basado en normas internacionales como ISO/IEC 27701, 27001, COBIT, entre otras. Se abordan etapas de diseño, implementación, monitoreo y mejora continua del sistema.
- **Técnico**
  Focalizado en la gestión y calibración de riesgos, identifica amenazas, vulnerabilidades, aplica métodos cuantitativos y cualitativos, y establece medidas de seguridad frente a ciberataques e incidentes.
- **Contenidos Sugeridos (No Obligatorios)**
  Se podrán considerar al menos uno de los siguientes métodos recomendados como: big data, machine learning, estrategias empresariales, compliance y herramientas de gestión.