Universidad® Ecotec

Programa Profesionalizante de Delegados de Protección de Datos Personales

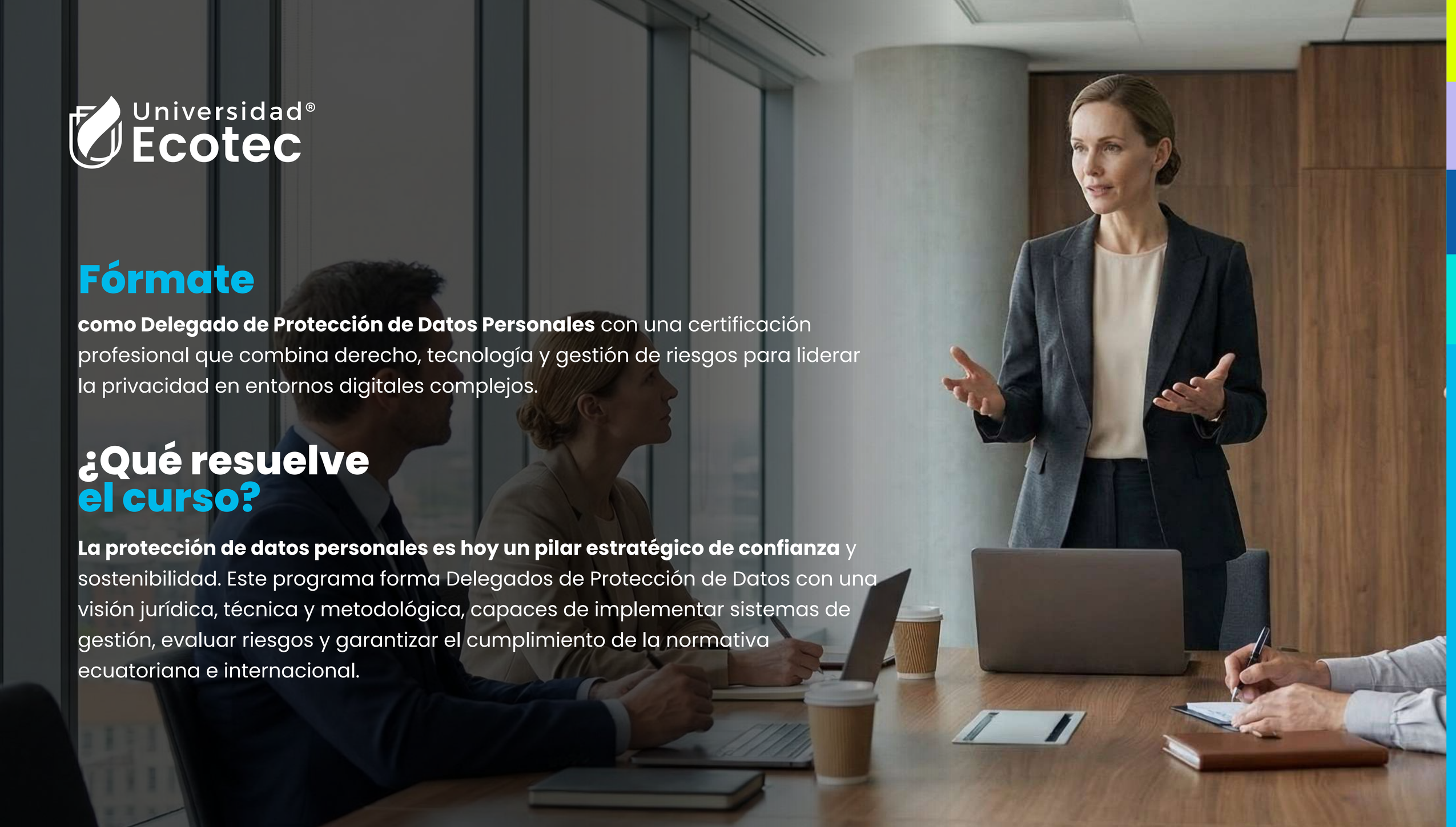
Universidad® Ecotec

Fórmate

como Delegado de Protección de Datos Personales con una certificación profesional que combina derecho, tecnología y gestión de riesgos para liderar la privacidad en entornos digitales complejos.

¿Qué resuelve el curso?

La protección de datos personales es hoy un pilar estratégico de confianza y sostenibilidad. Este programa forma Delegados de Protección de Datos con una visión jurídica, técnica y metodológica, capaces de implementar sistemas de gestión, evaluar riesgos y garantizar el cumplimiento de la normativa ecuatoriana e internacional.



Universidad® Ecotec

¿A quién está dirigido?

Pensado para abogados, auditores, compliance officers, oficiales de seguridad de la información y profesionales afines que tratan datos personales en Ecuador y necesitan asumir, fortalecer o profesionalizar el rol de Delegado de Protección de Datos Personales con respaldo normativo y técnico.

Al finalizar el curso podrás:

- **Interpretar y aplicar el marco jurídico de protección** de datos.
- **Implementar y gestionar Sistemas de Gestión** de Protección de Datos Personales.
- **Diseñar y aplicar metodologías de identificación,** evaluación y mitigación de riesgos.
- **Gestionar derechos de los titulares, transferencias** internacionales y brechas de seguridad.
- **Integrar estándares internacionales** (ISO, OWASP) al cumplimiento normativo.
- **Alinear la protección de datos con la estrategia,** la ética y la transparencia organizacional.

Universidad® Ecotec

Estructura modular

Módulo I

Derecho de protección de datos personales

Módulo II

Metodológico - Implementación de un Sistema de Gestión de Protección de Datos Personales

Módulo III

Técnico - Gestión de riesgos y Seguridad de datos

Módulo I

Contenido

Derecho de Protección de Datos Personales – 35 horas

1. Naturaleza jurídica
- Derecho de protección de datos: Constitución, ley, reglamento, resoluciones.
- Historia y evolución normativa del derecho a la protección de datos personales.
- Modelos de regulación mundial sobre protección de datos personales.
- Análisis del derecho a la protección de datos personales en el derecho constitucional ecuatoriano.
- Ética digital y objetivos de la Ley Orgánica de Protección de Datos Personales.
- Conceptos básicos de la Ley Orgánica de Protección de Datos Personales.
  - **i.** Datos personales.
  - **ii.** Titular.
  - **iii.** Tratamiento.
  - **iv.** Clasificación de los datos.
  - **v.** Transferencia.

2. Ámbito territorial y material de aplicación de la Ley Orgánica de Protección de Datos Personales.

3. Integrantes y roles del sistema de protección de datos personales.
- Titular.
- Responsables.
- Encargados.
- Delegados de Protección de Datos Personales.
- Terceros.
- Autoridad de Protección de Datos Personales.

4. Bases legitimadoras de tratamiento.
- Aplicación de cada base dependiendo de cada caso concreto.
- Validez del consentimiento (Art. 8 Ley Orgánica de Protección de Datos Personales).

5. Principios.
- Interpretación en tratamiento de datos personales.
- Aplicación en el tratamiento de datos personales.
- Responsabilidad proactiva y demostrada.
- Protección de datos personales desde el diseño y por defecto.

6. Finalidades del tratamiento.
- Objeto y Fundamentos prácticos.
- Tutela en el tratamiento de datos personales.

7. Derechos de los titulares de datos personales:
- Alcance de los derechos (énfasis en casos prácticos de datos sensibles).
- Excepciones a los derechos.
- Atención a los derechos.
- Canales de atención de derechos.
- Mecanismos de respuesta al ejercicio de derechos.
- Reglamento Denuncias vigente.
- Reglamento Consultas vigente.

8. Transferencias internacionales de datos personales:
- Nivel adecuado de protección.
- Garantías adecuadas, tales como: sellos, certificaciones y cláusulas contractuales tipo.
- Normas corporativas vinculantes.
- Autorización para ejecución.
- Excepcionalidades.
- Registro de información de Transferencias Internacionales.

9. Obligaciones con la Superintendencia de protección de Datos Personales de Responsables, Encargados, Terceros y Delegado de protección de datos personales.
- Notificaciones de brechas.
- Registros ante la autoridad.
- Denuncias.
- Ejercicio de derechos.
- Apoderados.

10. Régimen sancionador:
- Proceso Administrativo Sancionador.
- Infracciones Leves y Graves.
- Sanciones Leves y Graves.
- Responsabilidad administrativa y aproximación a otras responsabilidades.

11. Fenómenos culturales, tecnológicos y económicos en materia de protección de datos personales.

12. Protección de Datos y Estrategia Empresarial:
- Importancia de los datos personales del consumidor/usuario.
- Tratamiento de datos en análisis de mercado y elaboración de perfiles.
- Impacto reputacional y económico del cumplimiento normativo.

Módulo II

Metodológico - Implementación de un Sistema de Gestión de Protección de Datos Personales – 25 horas

1. Norma ISO/IEC 27001:2022 – Seguridad de la Información.

- Conceptos básicos de la norma (Confidencialidad, Integridad, Disponibilidad).
- Ciclo PDCA (Plan-Do-Check-Act) aplicado al SGSI.
- Controles relevantes de Anexo A vinculados a la privacidad (ej. gestión de accesos, cifrado, continuidad del negocio).
- Relación entre ISO 27001 y leyes de protección de datos.
- Mapeo de controles ISO 27001 y Ley de Protección de Datos Personales.

2. Norma ISO/IEC 27701:2019 - Gestión de la Privacidad (PIMS).

- Relación con ISO/IEC 27001 y 27002.
- Roles.
- Controles de privacidad
- Gestión del consentimiento, derechos de los titulares, transferencia internacional de datos.
- Estudio comparativo Ley de Protección de Datos Personales vs ISO 27701.

3. Norma ISO/IEC 29100 – Marco de Privacidad.

- Principios de privacidad: Consentimiento, minimización de datos, limitación de propósito, transparencia, responsabilidad.
- Actores: Sujeto de datos, controlador, procesador, terceros.
- Ciclo de vida de la información personal.
- Principios de privacidad en políticas empresariales.
- Brecha entre principios de privacidad y prácticas comerciales.

4. Mejor Practica OWASP ASVS (Application Security Verification Standard).

- Estructura de ASVS: Niveles básico, intermedio, avanzado.
- Controles de autenticación, autorización, gestión de sesión, criptografía, almacenamiento seguro de datos sensibles.
- Uso de ASVS como checklist en pruebas de seguridad.
- Requisitos de seguridad para aplicaciones que procesan datos personales.

5. Mejor Practica OWASP Top Ten.

- Principales vulnerabilidades:
- A01: Broken Access Control.
- A02: Cryptographic Failures.
- A03: Injection.
- A04: Insecure Design.
- A05: Security Misconfiguration.
- A06: Vulnerable and Outdated Components.
- A07: Identification & Authentication Failures.
- A08: Software and Data Integrity Failures.
- A09: Security Logging and Monitoring Failures.
- A10: Server-Side Request Forgery (SSRF).
- Relación con incidentes de filtración de datos.
- Mapeo de riesgos OWASP a controles de ISO 27001 e ISO 27701.

6. Inicio de la implementación un sistema de gestión de protección de datos personales.

- Iniciación.
- Análisis de controles existentes de seguridad de la información.
- Alcance.
- Aprobación y coordinación del plan.

7. Etapas de la Implementación (teórico y práctico):

- Definición y establecimiento.
  - **i.** Políticas de protección de datos personales.
  - **ii.** Gestión de riesgos para la protección de derechos y libertades.
    1. Establecimiento del contexto.
    2. Identificación de riesgos.
    3. Análisis de riesgos.
    4. Evaluación de riesgos.
    5. Tratamiento de riesgos.
  - **iii.** Evaluación de impacto de tratamiento de datos personales.
  - **iv.** Declaración de aplicabilidad (Justificar medidas de seguridad).
- Implementación.
  - **i.** Gestión de documental.
  - **ii.** Selección de medidas de seguridad, organizacionales y técnicas.
  - **iii.** Implementación.
  - **iv.** Capacitación y comunicación.
- Monitoreo y revisión
  - **i.** Análisis y evaluación del rendimiento del sistema.
  - **ii.** Auditorías internas y/o externas.
- Mantenimiento y mejora continua. Análisis y evaluación del rendimiento del sistema.
  - **i.** Tratamiento de no conformidades.
  - **ii.** Mejora continua e innovación.

Norma obligatoria de la Unidad II: Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales de la Superintendencia de Protección de Datos Personales.

Módulo III

Técnico – Gestión de Riesgos y Seguridad de Datos – 20 horas

1. Establecimiento del Contexto

- Planificación de la obtención de datos de entrada, elaboración de métricas, diseño de modelos de riesgo.
- Comprensión de los conceptos fundamentales de una gestión de riesgos para la protección de los derechos y libertades de los titulares de los datos.
- Elaboración de criterios de evaluación para la protección de derechos y libertades.
- Determinación de la tolerancia y/o de la capacidad al riesgo.

2. Implementación de la identificación de riesgos

- Perfilamiento de amenazas.
- Escaneo de vulnerabilidades técnicas y dependencias de software.
- Tipos de ciberataques (denegación de servicio, malware, entre otras).

3. Análisis cuantitativo de riesgo:

- Probabilidad de ocurrencia.
- Métodos frecuentistas, métodos Bayesianos u otros aplicables.
- Distribuciones de probabilidades (continuas y discretas).
- Modelos cuantitativos de riesgo.
  - **i.** FAIR (Factor Analysis of Information Risk).
  - **ii.** Análisis de Monte Carlo.
  - **iii.** Análisis de Markov.
- Ejemplos aplicables usando FAIR para el cálculo del Valor al riesgo en ciberseguridad y en protección de datos.
- Uso de análisis de Monte Carlo y/o Modelos de aprendizaje automático.
- Métodos de calibración a FAIR y ajuste en el cálculo de riesgo.

4. Priorización de riesgos: Estrategias y ponderación.

5. Implementación de medidas de seguridad en protección de datos personales:

- Medidas para la prevención de vulneraciones a la seguridad de datos personales.
- Medidas para la detección de vulneraciones a la seguridad de datos personales.
- Medidas para la respuesta a vulneraciones a la seguridad de datos personales.
- Interdependencias entre los controles de riesgos.
- Evaluación del rendimiento de las medidas de seguridad en el tiempo.
- Taxonomías de controles de riesgos (ISO/IEC 27001:2022)
  - **i.** Controles Organizativos (A.5) – 37 controles.
  - **ii.** Controles de Personas (A.6) – 8 controles.
  - **iii.** Controles Físicos (A.7) – 14 controles.
  - **iv.** Controles Tecnológicos (A.8) – 34 controles.
- Recuperación de desastres y continuidad de actividades (business continuity management).
- Respuesta a incidentes.

6. Relación de la tecnología con la protección de datos personales: Inteligencia Artificial:

- Conceptos de inteligencia artificial.
- Seguridad en el uso de inteligencia artificial para el cumplimiento de la ley de protección de datos personales.

Norma obligatoria de la Unidad III: Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales de la Superintendencia de Protección de Datos Personales.

Universidad® Ecotec

Universidad® Ecotec

Docentes

Luisa Gárate Rivera

Especialista en derecho digital, protección de datos y compliance, con experanormativa y docencia de posgrado.

Víctor Vera Anchundia

Especialista en seguridad informática, gestión de riesgos, DevSecOps y normativas ISO.

José Paúl Mendoza

Abogado experto en derecho digital, fintech y protección de datos, Subgerente Legal en banca digital y docente internacional.

Modalidad: **Online**

Incluye Certificado Digital con **Blockchain**

Duración: **80 horas**

Inicio del curso: **Marzo:** 3,4,5,10,11,12,17,18,19,24,25,26 y 31 - **Abril:** 1,7,8,9,14,15,16,21,22,23,28,29 y 30 - **Mayo:** 5

horarios: 18:30 a 21:30

Precio del curso
$700,00

Universidad®
Ecotec

Formación ejecutiva **con impacto real**