Modalidad: **e-learning**

Duración: **70 horas**
Fecha inicio: **27/01/2027**
Fecha final: **17/03/2027**

Programa Bonificable (FUNDAE)

Curso de Especialización

Ciberseguridad y resiliencia empresarial

Protege tu organización frente a los riesgos digitales y convierte el cumplimiento normativo en una ventaja estratégica

Con este curso lograrás...

- Comprender el **mapa normativo** europeo y español en materia de **seguridad de la información**, **ciberseguridad**, **resiliencia operativa digital** y **protección de datos** en su vertiente de seguridad.
- Identificar las **obligaciones exigibles a organizaciones** y **proveedores** de servicios derivadas del RGPD, la Directiva NIS2, DORA, el *Cyber Resilience Act* y el Reglamento de Inteligencia Artificial.
- Conocer el **Esquema Nacional de Seguridad** (ENS) como marco español de transposición de NIS2 y la norma ISO/IEC 27001 como estándar internacional de referencia para la gestión de la seguridad de la información.
- Conocer las **metodologías de gestión de riesgos** exigidas transversalmente por las principales normativas (NIS2, ENS, ISO 27001, DORA).
- Conocer las **exigencias** en materia de seguridad de la información cuando tu **compañía** es **proveedora** de productos o servicios.
- Anticipar las **novedades regulatorias** del *Cyber Resilience Act* (aplicable progresivamente entre 2026 y 2027) y del Reglamento de IA en lo relativo a sistemas de alto riesgo.

Este Curso para un seguimiento óptimo se acompañará de una **diversidad de recursos formativos** para conocer y comprender la totalidad de las problemáticas legales que supone la ciberseguridad y resiliencia empresarial mediante un diseño que resulte de utilidad tanto a quienes precisan asimilar desde sus fundamentos básicos, como a expertos que buscan completar sus conocimientos y centrarse en las novedades o en las cuestiones más polémicas o más discutidas.

Objetivos

- Interiorizar el **ecosistema normativo** europeo y nacional sobre seguridad de la información y resiliencia digital
- Dominar la **seguridad del RGPD**: medidas, evaluaciones de impacto y notificación de brechas.
- Analizar directiva **NIS2**, su transposición mediante el ENS y la ISO/IEC 27001 como referencia de **cumplimiento**.
- Comprender **DORA** y sus implicaciones para el sector financiero y sus proveedores TIC.
- Conocer las obligaciones de la ***Cyber Resilience Act*** y del **Reglamento de IA** para sistemas de **alto riesgo**.

Equipo Docente:

Jesús Yáñez Colomo

Socio de Privacidad, Cumplimiento Normativo y Ciberseguridad en Ecija. Cuenta con más de 20 años de experiencia en el asesoramiento técnico y jurídico en dichas áreas de práctica. Amplia trayectoria profesional, que inició en la filial de IBM en España y posteriormente al frente del área técnico-jurídica de la consultora Alaro Avant, Jesús ha liderado en los últimos años importantes proyectos de consultoría y asesoramiento jurídico con vocación internacional a grandes cuentas en materia de Seguridad Informática, *Compliance* y Nuevas Tecnologías. Especialista implantador SGSI (Aenor), especialista en Seguridad de Sistemas y Redes por la Universidad Nacional a Distancia (UNED) y ha sido reconocido por *Client Choice Awards* y *Best Lawyers* como mejor abogado en IT del mercado español. Además, cuenta con las certificaciones CISA, CISM, CDPSE, ITIL, 27001 *Lead Auditor*, *Europrise Legal & Technical Expert*.

Programa:

Módulo 1. RGPD/Seguridad de la información

- Medidas técnicas y organizativas apropiadas
- Notificación de brechas de seguridad y su comunicación al interesado
- Evaluación de impacto
- Responsabilidad proactiva y gestión del riesgo

Módulo 2. NIS2, ENS, ISO/IEC 27001

- Directiva NIS2/Directiva (UE) 2022/2555
- Esquema Nacional de Seguridad (ENS)/Real Decreto 311/2022
- ISO/IEC 27001 como estándar de referencia

Módulo 3. DORA. Resiliencia operativa digital del sector financiero

- Objeto y ámbito de aplicación. Marco de gestión del riesgo TIC
- Políticas de seguridad y notificación de incidentes y otras cuestiones
- Proveedores TIC terceros críticos
- Relación DORA/NIS2

Módulo 4. Gestión de riesgos de seguridad de la información

- Marco conceptual y requisitos normativos transversales
- Proceso de gestión de riesgos paso a paso
- Monitorización, revisión y mejora continua

Módulo 5. *Cyber Resilience Act* (CRA)

- Reglamento (UE) 2024/2847 sobre requisitos horizontales de ciberseguridad para productos con elementos digitales y su calendario de aplicación
- Ámbito de aplicación y sus requisitos esenciales de ciberseguridad
- Obligaciones de los fabricantes
- Productos importantes y críticos
- Impacto práctico para fabricantes, distribuidores e importadores de productos digitales

Módulo 6. Reglamento de Inteligencia Artificial. Sistemas de alto riesgo

- Reglamento (UE) 2024/1689 y su calendario de aplicabilidad
- Clasificación de sistemas de IA
- Obligaciones de los proveedores de sistemas de IA
- Sistemas de gestión de riesgos en IA.
- Requisitos y gobernanza de datos. Requisitos de ciberseguridad en sistemas IA.
- Obligaciones de los responsables del despliegue (deployers) de sistemas IA.

Metodología:

El Curso se imparte en modalidad **e-learning** en Campus Virtual de APD donde contarás para el seguimiento de la formación con una puesta a disposición de una variedad de **Recursos Formativos**:

- **Unidades Formativas** por Módulo
- Materiales **complementarios**
- **Foro de Docencia** con dinamizaciones y resoluciones de dudas por **Docentes Expertos**
- **Casos prácticos** resueltos
- **Vídeos** de los Docentes Expertos por cada Módulo
- **Encuentros digitales en tiempo real** que se facilitan posteriormente en formato vídeo

Contarás, además, con el apoyo de nuestro **equipo docente** a través de una coordinación académica que te orientará de forma continua para que alcances el aprovechamiento máximo con esta formación con una planificación por Módulo semanal y una última semana de cierre. Así, junto a tu **aprendizaje individual** conseguirás también un **aprendizaje colaborativo** a través de la interactuación con nuestros Docentes Expertos y los profesionales que te acompañarán mediante la interacción, el diálogo y la resolución práctica de dudas.

Contarás con:

Foros

El curso dispone de dos foros de carácter consultivo: el **Foro de Docencia** y el **Foro de Ayuda**. Estos foros desempeñarán un papel fundamental en el seguimiento del curso, ya que permitirán la resolución de dudas, el intercambio de impresiones y la puesta en común de las dificultades que puedan surgir a medida que avance la formación.

Además, el equipo docente participará activamente mediante una dinamización semanal orientada a reforzar los contenidos y a incorporar, cuando sea pertinente, novedades relevantes sobre la temática.

Encuentros Digitales

Realizados en **tiempo real** y que estarán programados desde el comienzo del Curso para poder organizar tu agenda con antelación, siendo impartidos por el **Docente Experto**, donde siempre se reservará un espacio para preguntas de participantes.

Además, estos Encuentros serán grabados y puestos a disposición del alumnado en el campus para poder ser visionados con posterioridad al editarse en formato vídeo.

Dirigido a:

Profesionales integrados en departamentos jurídico, *compliance*, seguridad de la información (CISOs), tecnología, protección de datos, auditoría interna y dirección general.

Socios Globales **735 €** +IVA
Socios Protectores **588 €** +IVA

INSCRIBIRSE AHORA

¿Te interesa este curso y no eres socio de APD? Entonces ponte en contacto con nosotros dirigiéndote a este correo electrónico: Alicia Calderón | **acalderon@apd.es**