

Tema I	Introducción: Ordenamiento jurídico Nacional, Comunitario e Internacional Protección de datos en España Derecho Comparado: ordenamiento jurídico comunitario e internacional. Estándares y buenas prácticas Ámbito de aplicación objetivo, subjetivo y territorial.
Tema II	RGDP: Principios y Legitimación Principios de aplicación a las actividades de tratamiento: licitud, lealtad, transparencia, exactitud, minimización y limitación de la finalidad. El consentimiento como base de legitimación de las actividades de tratamiento. Supuestos particulares. Bases jurídicas distintas del consentimiento.
Tema III	RGDP: Derechos de los Individuos Transparencia e información. Acceso, rectificación, supresión (olvido). Oposición. Decisiones individuales automatizadas. Portabilidad. Limitación del tratamiento. Excepciones a los derechos.
Tema IV	RGDP: Medidas de Cumplimiento y Responsabilidad Proactiva Las políticas de protección de datos. Relación y regulación con terceros intervinientes en las actividades de tratamiento. El registro interno de actividades de tratamiento. Privacidad desde el diseño y por defecto. Evaluación de impacto relativa a protección de datos. Seguridad de los sistemas de información – <i>técnica y organizativa</i> -. Violaciones de seguridad. Códigos de conducta y certificaciones.
Tema V	RGDP: Delegado de Protección de Datos Designación. Proceso de toma de decisiones. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses. Obligaciones y responsabilidades. Independencia. Identificación y reporte a dirección. Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones. Comunicación con la Autoridad de control. Competencia profesional. Negociación. Comunicación. Presupuestos. Formación. Habilidades personales, trabajo en equipo, liderazgo, gestión de equipos.
Tema VI	RGDP: Transferencias Internacionales de Datos El sistema de decisiones de adecuación. Transferencias mediante garantías adecuadas. Normas Corporativas Vinculantes. Cláusulas contractuales. Excepciones. Autorización de la autoridad de control. Suspensión temporal.
Tema VII	RGDP: Las Autoridades de Control Autoridades de Control. Potestades. Régimen sancionador. Comité Europeo de Protección de Datos. Procedimientos seguidos por la AEPD. La tutela jurisdiccional. El derecho de indemnización.
Tema VIII	La Transversalidad de la Protección de Datos Sectores y particularidades: sanitario, farmacéutico, investigación, servicios sociales, solvencia patrimonial, telecomunicaciones, financiero – seguros, publicidad, abogacía y seguridad. Normativas con implicaciones: prevención del blanqueo de capitales y financiación del terrorismo, responsabilidad penal de las personas jurídicas, servicios de la sociedad de la información y del comercio electrónico, firma electrónica, transparencia.
Tema IX	Análisis y Gestión de Riesgos de los Tratamientos. Evaluaciones de Impacto de Protección de Datos Introducción. Marco y conceptos generales. Evaluación de riesgos. Inventario y valoración de activos, Inventario y valoración amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante. Gestión de riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo asumible. Metodologías de análisis y gestión de riesgos. Realización de una evaluación de impacto. Aspectos preparatorios y organizativos, análisis de la necesidad de llevar a cabo la evaluación y consultas previas.
Tema X	Programas de Cumplimiento y Seguridad de la Información El diseño y la implantación del programa de protección de datos en el contexto de la organización. Trabajos de integración de sistemas. Accountability: la trazabilidad del modelo de cumplimiento.
Tema XI	Seguridad de la Información Marco normativo. Esquema Nacional de Seguridad y Directiva NIS: Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión. Ámbito de aplicación, objetivos, elementos principales, principios básicos y requisitos mínimos. Ciberseguridad y gobierno de la seguridad de la información. Generalidades, misión, gobierno efectivo de la Seguridad de la Información (SI). Conceptos SI. Alcance. Métricas del gobierno de la SI. Estado de la SI. Estrategia de SI. Puesta en práctica de la seguridad de la información. Seguridad desde el diseño y por defecto. El ciclo de vida de los sistemas de información. Integración de la seguridad y la privacidad en el ciclo de vida. El control de calidad de los SI.
Tema XII	Auditoría de Protección de Datos Proceso de auditoría. Elaboración del Informe de Auditoría. Ejecución y seguimiento de acciones correctoras.
Tema XIII	Auditoría de Sistemas de Información Objetivos. Conceptos básicos. Estándares y Directrices de Auditoría de SI. Control interno y mejora continua. Buenas prácticas. Integración de la auditoría de protección de datos en la auditoría de SI. Planificación, ejecución y seguimiento.
Tema XIV	Gestión de la Seguridad de Información Esquema Nacional de Seguridad. ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014; Requisitos de Sistemas de Gestión de Seguridad de la Información – SGSI. Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación. Recuperación de desastres y continuidad del negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la recuperación de desastres.
Tema XV	Protección de datos en el Mundo Digital Impacto de los desarrollos tecnológicos en la protección de datos: cloud computing; smartphones; IoT, Big Data y elaboración de perfiles, RRSS, Geolocalización, Blockchain. Dificultades de aplicación de la Normativa. Mecanismos de mitigación.