

TEMARIO

Organiza

csc
CYBER SECURITY CENTRE

dpi
DATA PRIVACY INSTITUTE

Curso Cyber Compliance:
adecuación al nuevo marco
normativo de la Ciberseguridad

isms
FORUM

INTERNATIONAL
INFORMATION
SECURITY
COMMUNITY

Dominio	Temas	Horas	
1. Presentación del Curso.	Introducción al CyberCompliance	1	
1.2 Ciberpolítica internacional,	Política legislativa en materia Ciber y Estrategia Nacional de Ciberseguridad	1	
Ámbito del CyberCompliance	a) Framework sobre Identidad digital y Firma Electrónica. Normativa eIDAS b) Normativa sectorial Telco: Seguridad 5G, retención de datos, cadena de suministro, etc.	2	
	c) Normativa sectorial financiera: DORA, EIOPA, normativa externalización de BCE y Banco de España, SWIFT, etc..	2	
	d) ENS	1	
	2.1. Normativa	e) Procedimientos de Third Party Compliance	1
		f) Roles, competencias y Gobierno: CISO, DPO, Compliance, Auditoría, Asesoría Jurídica, Riesgos, etc.	1
		g) Seguridad en redes e infraestructuras: NIS2, LPIC, Directiva de resiliencia de entidades críticas, Propuesta de Reglamento de Ciberresiliencia (CRA), dedicado a la ciberseguridad de los productos (hardware y software). h) Instituciones, Autoridades de Control y Competencias: Ministerios, INCIBE, CCN, CNPIC, AEPD, EDPS, ENISA, etc. Regímenes de infracciones y sanciones.	4
		i) Protección de Activos intangibles, Propiedad intelectual e industrial, secretos empresariales y algoritmos. El Reglamento de IA	3
		2.2. Estándares y Buenas Prácticas	a) Procedimientos internos: riesgos tecnológicos con proveedores, clasificación de información, seguridad Cloud, Gestión de incidentes de seguridad, etc.
b) Obligaciones contractuales en materia de ciberseguridad	1		
c) ISO 31000 y 31022 d) ISO 37301	2		
e) ISO 27701 (privacidad) e ISO 31700 (privacy by design)	1		
3. Metodologías de riesgo legal y claves para la implantación de sistemas de gestión de cumplimiento	3.1. Observatorio normativo y Legal risk mapping		1
	3.2. Análisis de riesgos legales	2	
	3.3. Creación de Cultura Compliance y generación de indicadores de Cumplimiento		
	3.4. Plan de CyberCompliance, medidas, controles, desempeño, indicadores, etc.	1	
	3.5. Modelo de Gobierno de CyberCompliance, responsabilidades, estructura, nombramientos y figuras. Competencias y roles. Accountability	1	
4. Auditoría de CyberCompliance.	Modelos de Supervisión. Actividad Forense y gestión de evidencias	2	
5. Ciberdelincuencia en la empresa	Investigaciones y Aspectos procesales. Modelo de prevención de delitos ciber	2	