TEMARIO CURSO CYBER COMPLIANCE: ADAPTACIÓN AL NUEVO MARCO NORMATIVO DE LA CIBERSEGURIDAD

Dominio	Subdominio	Apartados
1. Presentación del Curso. Introducción al CyberCompliance		
1. Ciberpolítica internacional, Política legislativa en materia Ciber y Estrategia Nacional de Ciberseguridad		
2. Ámbito del CyberCompliance	2.1. Normativa	a) Framework sobre Identidad digital y Firma Electrónica. Normativa eIDAS
		b) Normativa sectorial Telco: Seguridad 5G, retención de datos, cadena de suministro, etc.
		c) Normativa sectorial financiera: DORA, EIOPA, normativa externalización de BCE y Banco de España, SWIFT, etc..
2. Ámbito del CyberCompliance	2.1. Normativa	d) 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). Desarrollo del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (EUCSA)
		e) ENS
	2.1. Normativa	f) Instituciones, Autoridades de Control y Competencias: Ministerios, INCIBE, CCN, CNPIC, AEPD, EDPS, ENISA, etc. Regímenes de infracciones y sanciones.
	2.1. Normativa	g) Procedimientos de Third Party Compliance

TEMARIO CURSO CYBER COMPLIANCE: ADAPTACIÓN AL NUEVO MARCO NORMATIVO DE LA CIBERSEGURIDAD

Sesión 3	**2. Ámbito del CyberCompliance**	2.1. Normativa	h) Protección de Activos intangibles, Propiedad intelectual e industrial, secretos empresariales y algoritmos. El Reglamento de IA
			i) Privacidad y Protección de Datos
		2.2. Framework normativo interno	a) Procedimientos internos: riesgos tecnológicos con proveedores, clasificación de información, seguridad Cloud, Gestión de incidentes de seguridad, etc.
Sesión 4	**2. Ámbito del CyberCompliance**	2.2. Framework normativo interno	b) Roles, competencias y Gobierno: CISO, DPO, Compliance, Auditoría, Asesoría Jurídica, Riesgos, etc.
		2.2. Framework normativo interno	c) Obligaciones contractuales en materia de ciberseguridad
		2.3. Estándares y Buenas Prácticas	a) ISO 31000 y 31002
			b) ISO 37301
			c) ISO 27001
			d) ISO 27701 (privacidad) e ISO 31700 (privacy by design)
Sesión 5	**3. Metodologías de riesgo legal y claves para la implantación de sistemas de gestión de cumplimiento**	3.1. Observatorio normativo y Legal risk mapping	
		3.2. Análisis de riesgos legales	
Sesión 6	**3. Metodologías de riesgo legal y claves para la implantación de sistemas de gestión de cumplimiento**	3.3. Plan de CyberCompliance, medidas, controles, desempeño, indicadores, etc.	
		3.4. Modelo de Gobierno de CyberComplliance, responsabilidades, estructura, nombramientos y figuras. Competencias y roles. Accountability	
Sesión 7	**3. Metodologías de riesgo legal y claves para la implantación de sistemas de gestión de cumplimiento**	3.5. Creación de Cultura Compliance y generación de indicadores de Cumplimiento	
	4. Auditoría de CyberCompliance. Modelos de Supervisión. Activida Forense y gestión de evidencias		
Sesión 8	**5. Ciberdelincuencia en la empresa: Investigaciones y Aspectos procesales. Modelo de prevención de delitos ciber**		