CONTENIDOS DE LA UNIDAD, CRITERIOS DE EVALUACIÓN Y RESULTADOS DE APRENDIZAJE

La siguiente tabla responde al REAL DECRETO 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo. Se incluye también una columna con las unidades didácticas que forman el curso, en las que se desarrollas los diferentes bloques de contenidos.

CONTENIDOS	CRITERIOS DE EVALUACIÓN	RESULTADOS DE APRENDIZAJE	UNIDAD DIDÁCTICA
Bloque 1			
Puntos principales de aplicación para un correcto cumplimiento normativo: • Introducción al cumplimiento normativo (Compliance: objetivo, definición y conceptos principales). • Principios del buen gobierno y ética empresarial. • Compliance Officer: funciones y responsabilidades. • Relaciones con terceras partes dentro del Compliance.	a) Se han identificado las bases del cumplimiento normativo a tener en cuenta en las organizaciones. b) Se han descrito y aplicado los principios de un buen gobierno y su relación con la ética profesional. c) Se han definido las políticas y procedimientos, así como la estructura organizativa que establezca la cultura del cumplimiento normativo dentro de las organizaciones. d) Se han descrito las funciones o competencias del responsable del cumplimiento normativo dentro de las organizaciones. e) Se han establecido las relaciones con terceros para un correcto cumplimiento normativo	1. Identifica los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades	1
Bloque 2			
Diseño de sistemas de cumplimiento normativo: • Sistemas de Gestión de Compliance. • Entorno regulatorio de aplicación. • Análisis y gestión de riesgos, mapas de riesgos.	a) Se han recogido las principales normativas que afectan a los diferentes tipos de organizaciones. b) Se han establecido las recomendaciones válidas para diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 19.600 entre otras). c) Se han realizado análisis y evaluaciones de los riesgos de diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 31.000 entre otras).	2. Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.	2

• Documentación del sistema de cumplimiento normativo diseñado.	d) Se ha documentado el sistema de cumplimiento normativo diseñado.		
Bloque 3			
Legislación para el cumplimiento de la responsabilidad penal: • Riesgos penales que afectan a la organización. • Sistemas de gestión de Compliance penal. • Sistemas de gestión anticorrupción.	a) Se han identificado los riesgos penales aplicables a diferentes organizaciones. b) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados. c) Se ha establecido un sistema de gestión de cumplimiento normativo penal de acuerdo con la legislación y normativa vigente (Código Penal y UNE 19.601, entre otros). d) Se han determinado los principios básicos dentro de las organizaciones para combatir el soborno y promover una cultura empresarial ética de acuerdo con la legislación y normativa vigente (ISO 37.001 entre otros).	3. Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.	3
Bloque 4			
Legislación y jurisprudencia en materia de protección de datos: • Principios de protección de datos. • Novedades del RGPD de la Unión Europea. • Privacidad por Diseño y por Defecto. • Análisis de Impacto en Privacidad (PIA), y medidas de seguridad. • Delegado de Protección de Datos (DPO).	a) Se han reconocido las fuentes del Derecho de acuerdo con el ordenamiento jurídico en materia de protección de datos de carácter personal. b) Se han aplicado los principios relacionados con la protección de datos de carácter personal tanto a nivel nacional como internacional. c) Se han establecido los requisitos necesarios para afrontar la privacidad desde las bases del diseño. d) Se han configurado las herramientas corporativas contemplando el cumplimiento normativo por defecto. e) Se ha realizado un análisis de riesgos para el tratamiento de los derechos a la protección de datos. f) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos	4. Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.	4

	identificados en la protección de datos. g) Se han descrito las funciones o competencias del delegado de protección de datos dentro de las organizaciones.		
Bloque 5			
Normativa vigente de ciberseguridad de ámbito nacional e internacional: • Normas nacionales e internacionales. • Sistema de Gestión de Seguridad de la Información (estándares internacionales) • (ISO 27.001). • Acceso electrónico de los ciudadanos a los Servicios Públicos. • Esquema Nacional de Seguridad (ENS). • Planes de Continuidad de Negocio (estándares internacionales) (ISO 22.301). • Directiva NIS. • Legislación sobre la protección de infraestructuras críticas. • Ley PIC (Protección de infraestructuras críticas).	a) Se ha establecido el plan de revisiones de la normativa, jurisprudencia, notificaciones, etc. jurídicas que puedan afectar a la organización. b) Se ha detectado nueva normativa consultando las bases de datos jurídicas siguiendo el plan de revisiones establecido. c) Se ha analizado la nueva normativa para determinar si aplica a la actividad de la organización. d) Se ha incluido en el plan de revisiones las modificaciones necesarias, sobre la nueva normativa aplicable a la organización, para un correcto cumplimiento normativo. e) Se han determinado e implementado los controles necesarios para garantizar el correcto cumplimiento normativo de las nuevas normativas. incluidas en el plan de revisiones.	5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.	5

Este módulo profesional contiene la formación necesaria para desempeñar la función de diseñar el sistema de cumplimiento normativo de ciberseguridad en una organización.

La función de diseñar un sistema de cumplimiento normativo incluye aspectos como la caracterización de los principales aspectos de las diferentes normativas de ciberseguridad de obligado cumplimiento para la organización.

Las actividades profesionales asociadas a esta función se aplican en la integración, de las últimas actualizaciones en normativa de ciberseguridad a nivel nacional e internacional que apliquen, en el sistema de cumplimiento normativo de la organización.