

# Curso Cyber Compliance: adecuación ao novo marco normativo da Ciberseguridade

## Descrición

Ofrece unha visión completa e detallada do marco legal e regulatorio da Ciberseguridade, así como da importancia do cumprimento normativo na contorna dixital actual. Co obxectivo de proporcionar unha formación práctica e completa, o curso divídese en cinco bloques temáticos que abarcan desde a normativa e os estándares internacionais, ata as metodoloxías de risco legal e as claves para a implantación de sistemas de xestión de cumprimento.

## Obxectivos

- Comprender o marco normativo nacional e internacional aplicable á ciberseguridade e o CyberCompliance.
- Aplicar estándares, boas prácticas e metodoloxías para a xestión de riscos legais e cumprimento normativo.
- Desenvolver competencias para implementar, auditar e supervisar sistemas de xestión de CyberCompliance en organizacións.

### HORARIO

- . 17 de novembro e 3 de decembro de 16:00 a 18:00 horas
- . 19 de novembro e 1 de decembro de 16:00 a 19:00 horas
- . 18, 24, 25 e 26 de novembro e 2 de decembro de 16:00 a 20:00 horas

## Dirixido a

- Directores/as de seguridade da Información
- Consultores/as
- Avogadosas
- Auditores/as
- Técnicos/as de seguridade
- Técnicos/as de sistemas con responsabilidades de seguridade

### BENEFICIOS

Diploma de asistencia

Opción gratuita dun exame de certificación oficial

## Perfil do docente

A formación contará cun equipo docente de referencia nacional e internacional, composto por profesionais cunha sólida traxectoria en ciberseguridade, privacidade, cumprimento normativo, resiliencia dixital e dereito tecnolóxico. Este grupo multidisciplinar achega unha combinación única de experiencia técnica, visión estratéxica, liderado institucional e capacidade divulgativa, garantindo unha formación rigorosa, actualizada e aliñada cos retos reais do entorno dixital.

### PROGRAMA

Programación 2025/26

### TIPO

CURSO

### MATRÍCULA

Gratuíta

### PERIODO INSCRICIÓN

20/10/2025 - 02/11/2025

### PROBA DE SELECCIÓN

06/11/2025 (17:30)

### CRITERIOS DE SELECCIÓN

Proba técnica presencial no CNTG en Santiago de Compostela

### Nº PRAZAS

16 (Mínimo 10)

### METODOLOXÍA

Virtual

<b>TIPO DE EDICIÓN</b>	Edición única (desempregados/as e ocupados/as)
<b>DURACIÓN</b>	30 horas
<b>DATA INICIO</b>	17/11/2025
<b>DATA FIN</b>	03/12/2025
<b>HORARIO</b>	. 17 de novembro e 3 de decembro de 16:00 a 18:00 horas
<b>LUGAR DE DOCENCIA</b>	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
<b>CERTIFICACIÓN OFICIAL</b>	Sí
<b>EXAME CERTIFICACIÓN</b>	Certified Professional Cyber Compliance (CPCC)
<b>MÓDULOS TRANSVERSAIS</b>	Igualdade de 5 horas
<b>TECNOLOXÍA</b>	ISMS Forum  Ciberseguridade/Ciberseguridade
<b>PERIODO DOCENCIA</b>	17/11/2025 - 03/12/2025

## Temario

1. Introducción ao CyberCompliance
  - 1.1 Presentación do Curso.
  - 1.2 Ciberpolítica internacional, Política lexislativa en materia Ciber e Estratexia Nacional de Ciberseguridade
2. Ámbito do CyberCompliance
  - 2.1 Normativa
    - a) Framework sobre Identidade dixital e Firma Electrónica. Normativa eIDAS
    - b) Normativa sectorial Telco: Seguridade 5G, retención de datos, cadea de subministración etc.
    - c) Normativa sectorial financeira: DOURA, EIOPA, normativa externalización de BCE e Banco

de España, SWIFT etc..

d) ENS

e) Procedementos de Third Party Compliance

f) Roles, competencias e Goberno: CISO, DPO, Compliance, Auditoría, Asesoría Xurídica, Riscos etc.

g) Seguridade en redes e infraestruturas: NIS2, LPIC, Directiva de resiliencia de entidades críticas, Proposta de Regulamento de Ciberresiliencia (CRA), dedicado á ciberseguridade dos produtos (hardware e software).

h) Institucións, Autoridades de Control e Competencias: Ministerios, INCIBE, CCN, CNPIC, AEPD, EDPS, ENISA etc. Réximes de infraccións e sancións.

i) Protección de Activos intanxibles, Propiedade intelectual e industrial, segredos empresariais e algoritmos. O Regulamento de IA

## 2.2. Estándares e Boas Prácticas

a) Procedementos internos: riscos tecnolóxicos con provedores, clasificación de información, seguridade Cloud, Xestión de incidentes de seguridade etc.

b) Obrigacións contractuais en materia de ciberseguridade

c) ISO 31000 e 31022 d) ISO 37301

e) ISO 27701 (privacidade) e ISO 31700 (privacy by design)

## 3. Metodoloxías de risco legal e claves para a implantación de sistemas de xestión de cumprimento

3.1 Observatorio normativo e Legal risk mapping

3.2. Análise de riscos legais

3.3. Creación de Cultura Compliance e xeración de indicadores de Cumprimento

3.4. Plan de CyberCompliance, medidas, controis, desempeño, indicadores, etc.

4. Auditoría de CyberCompliance.

Modelos de Supervisión. Actividade Forense e xestión de evidencias

## 5. Ciberdelincuencia na empresa

Investigacións e Aspectos procesuais. Modelo de prevención de delitos ciber