

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.

HORARIO

. 16 e 25 de novembro de 16:00 a 18:00 horas

. 18 e 24 de novembro de 16:00 a 19:00 horas

. 17, 23, 30 de novembro, 1 e 2 de decembro de 16:00 a 20:00 horas

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.

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

Opción gratuita dun exame de certificación oficial

Diploma de asistencia

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 2026/27

TIPO

CURSO

MATRÍCULA

Gratuíta

PERIODO INSCRICIÓN

01/10/2026 - 15/10/2026

PROBA DE SELECCIÓN

16/10/2026 (00:00)

CRITERIOS DE SELECCIÓN

Proba técnica presencial no CNTG en Santiago de Compostela

Nº PRAZAS

16 (Mínimo 10)

METODOLOXÍA

Virtual



TIPO DE EDICIÓN	Edición única tarde (desempregados/as e ocupados/as)
DURACIÓN	30 horas
DATA INICIO	16/11/2026
DATA FIN	02/12/2026
HORARIO	Horario de referencia: de luns a mércores de 16.00 a 20.00
LUGAR DE DOCENCIA	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	Certified Professional Cyber Compliance (CPCC)
MÓDULOS TRANSVERSAIS	Igualdade de 5 horas
TECNOLOXÍA	Ciberseguridade/Ciberseguridad ISMS Forum
PERIODO DOCENCIA	16/11/2026 - 02/12/2026

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