

Curso de Goberno en Ciberseguridade

Descrición

Ofrece profundos coñecementos sobre os fundamentos e goberno da ciberseguridade, arquitecturas, políticas, estratexia e estándares, análises e xestión de riscos, marco normativo, operativa de ciberseguridade, infraestruturas críticas, ciberinteligencia, xestión de incidentes, boas prácticas e soft skills da figura do/a Director/a de Seguridade da Información.

Obxectivos

- Adquirir coñecementos sólidos en goberno, xestión de riscos e cumprimento legal en ciberseguridade.
- Desenvolver habilidades técnicas en análises de vulnerabilidades, criptografía, hacking ético e resposta a incidentes.
- Fortalecer competencias estratéxicas e operativas para liderar a ciberseguridade en entornos complexos e críticos.

Dirixido a

- Directores/as de seguridade da Información
- Consultores/as
- Avogados/as
- Auditores/as
- Técnicos/as de seguridade
- Técnicos/as de sistemas con responsabilidades na seguridade e de sistemas

BENEFICIOS

Diploma de asistencia

Opción gratuita dun exame de certificación oficial

Perfil do docente

O equipo docente que participa nesta formación está composto por profesionais altamente cualificados en ciberseguridade, privacidade, cumprimento normativo, xestión de riscos e tecnoloxías emerxentes. Procedentes de distintos sectores —incluíndo a administración pública, a banca, a consultoría, a industria e o ámbito académico—, estes/as expertos/as achegan unha visión transversal e actualizada sobre os desafíos que afrontan as

Curso de Goberno en Ciberseguridade

organizacións na contorna dixital.

A diversidade de especializacións e traxectorias permite abordar a formación desde múltiples perspectivas: técnica, xurídica, estratéxica e operativa. Ao longo do programa, trataranse temas clave como a protección de datos, a ciberresiliencia, a seguridade en infraestruturas críticas, o goberno da seguridade na nube, e a adaptación aos marcos regulatorios europeos e internacionais.

| | |
|-------------------------------|---|
| PROGRAMA | Programación 2025/26 |
| TIPO | CURSO |
| MATRÍCULA | Gratuíta |
| PERIODO INSCRICIÓN | 02/02/2026 - 15/02/2026 |
| PROBA DE SELECCIÓN | 18/02/2026 (18:30) |
| CRITERIOS DE SELECCIÓN | Proba técnica presencial no CNTG en Santiago de Compostela |
| Nº PRAZAS | 16 (Mínimo 10) |
| METODOLOXÍA | Virtual |
| TIPO DE EDICIÓN | Edición única (desempregados/as e ocupados/as) |
| DURACIÓN | 46 horas |
| DATA INICIO | 02/03/2026 |
| DATA FIN | 25/03/2026 |
| HORARIO | De luns a mércores de 16:00 a 20:00 horas (último día ata as |
| LUGAR DE DOCENCIA | Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en |

| | |
|------------------------------|--|
| CERTIFICACIÓN OFICIAL | Sí |
| EXAME CERTIFICACIÓN | Certified Cyber Security Professional (CCSP) |
| MÓDULOS TRANSVERSAIS | Igualdade de 5 horas |
| TECNOLOXÍA | Ciberseguridade/Ciberseguridad ISMS Forum |
| PERIODO DOCENCIA | 02/03/2026 - 25/03/2026 |

Temario

1 - GOBERNO DE SEGURIDADE

- 1.1 Arquitecturas de Seguridade
- 1.2 e 1.3 Introducción e Xestión de Ciberseguridade
- 1.4 Organización Roles e Responsabilidades
- 1.5 Goberno de ciberseguridade
- 1.6 Auditoría e control da seguridade
- 1.7 Certificación e acreditación de produtos e sistemas
- 1.8 Seguridade en contornas Cloud (IaaS, PaaS, SaaS) Modelos e Controis esixibles

2 - ANÁLISE E XESTIÓN DE RISCOS

- 2.1 Identificación e xestión de riscos
- 2.2 Análise e xestión de riscos e ameazas
- 2.3 Riscos Tecnolóxicos

3 - CUMPRIMENTO LEGAL E NORMATIVO

- 3.1 Cumprimento legal
- 3.2 Aspectos legais e regulatorios asociados a Privacidade, Seguridade, e IC
- 3.3 Técnicas, metodoloxías e ferramentas do cumprimento legal
- 3.4 Notificación, reporte, denuncia e presentación en xulgado
- 3.5 Cibercrime e delitos informáticos

4 - OPERATIVA DE CIBERSEGURIDADE

- 4.1 Desenvolvemento seguro
- 4.2 Criptografía
- 4.3 Monitorización de seguridade

- 4.4 Tecnoloxías de ciberseguridade
- 4.5 e 4.6 Análise de vulnerabilidades e Hacking ético
- 4.7 Seguridade do Directo Activo e parque Windows. Directivas e GPOs Configuración segura
- Modelos de capas TIER Recomendacións de seguridade
- 4.8 Seguridade no acceso remoto e o teletraballo

5 - CIBER INTELIXENCIA, COOPERACIÓN E CAPACIDADE

- 5.1 Relacións con organismos nacionais e internacionais
- 5.2 Ciber Exercicios
- 5.3 Intercambio de información con terceiros e IoCs

6 - XESTIÓN EFICAZ DE INCIDENTES

- 6.1 Análise Forense de Sistemas
- 6.2 Análise de malware
- 6.3 Xestión e resposta a incidentes de Seguridade

7 - INFRAESTRUTURAS CRÍTICAS

- 7.1 Ciberseguridade en IC
- 7.2 OT e IoT

8 - CISO SOFTSKIILLS

- 8.1 Estratexia de Seguridade
- 8.2 Planificación dunha xestión de Crise
- 8.3 Softskills

Simulacro de exame e corrección