



CYBER SECURITY CENTRE

**TEMARIO DEL
CURSO DE ESPECIALIZACIÓN
EN CIBERSEGURIDAD**

CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD

| DOMINIO | ID | TEMA |
|--|--|---|
| 1 GOBIERNO DE SEGURIDAD | 1 | Arquitecturas de Seguridad |
| | 2 | Introducción y Gestión de Ciberseguridad |
| | 3 | |
| | 4 | |
| | 5 | Organización Roles y Responsabilidades |
| | 6 | Gobierno de ciberseguridad |
| | 7 | Auditoría y control de la seguridad |
| | 8 | Certificación y acreditación de productos y sistemas |
| 2 ANÁLISIS Y GESTIÓN DE RIESGOS | 8 | Seguridad en entornos Cloud (IaaS, PaaS, SaaS) |
| | | Modelos |
| | | Controles exigibles |
| 3 CUMPLIMIENTO LEGAL Y NORMATIVO | 9 | La identificación y gestión de riesgos |
| | 10 | Análisis y gestión de riesgos y amenazas |
| | 11 | Riesgos Tecnológicos |
| 3 CUMPLIMIENTO LEGAL Y NORMATIVO | 12 | Cumplimiento Legal |
| | 13 | Aspectos legales y regulatorios asociados a Privacidad, Seguridad, e IC |
| | 14 | Técnicas, metodologías y herramientas del compliance legal |
| | 15 | Notificación, reporte, denuncia y presentación en juzgado |
| | 16 | Cibercrimen y delitos informáticos |
| 4 OPERATIVA DE CIBERSEGURIDAD | 17 | Desarrollo seguro |
| | 18 | Criptografía |
| | 19 | Monitorización de seguridad |
| | 20 | Tecnologías de ciberseguridad |
| | 21 | Análisis de vulnerabilidades |
| | 22 | Hacking ético |
| | 23 | Seguridad del Directo Activo y parque Windows |
| | | Directivas y GPOs |
| | | Configuración segura |
| | | Modelos de capas TIER |
| | | Recomendaciones de seguridad |
| | 24 | Seguridad en el acceso Remoto y el teletrabajo. |
| | Roles: Usuarios privilegiados | |
| | Roles: Elevación de privilegios | |
| | Acceso remoto: Modalidades | |
| | Acceso remoto: Cumplimiento y su problemática en el acceso directo a | |
| | Acceso remoto: Acceso Seguro a | |
| | Puestos remotizados y VDIs: | |
| | Arquitectura | |
| | Puestos remotizados y VDIs: Ventajas e inconvenientes | |
| 5 CIBER INTELIGENCIA, COOPERACIÓN Y CAPACIDAD | 25 | Relaciones con organismos nacionales e Internacionales |
| | 26 | Ciber Ejercicios |
| | 27 | Intercambio de información con terceros e IoCs |
| 6 GESTIÓN EFICAZ DE INCIDENTES | 28 | Análisis Forense de Sistemas |
| | 29 | Análisis de malware |
| | 30 | Gestión y respuesta a incidentes de Seguridad |
| 7 INFRAESTRUCTURAS CRITICAS | 31 | Ciberseguridad en IC |
| | 32 | OT e IoT |
| 8 CISO Soft Skills | 33 | Estrategia de Seguridad |
| | 34 | Planificación de una gestión de Crisis |
| | 35 | Softskills |
| 9 Sesión práctica y simulacro de examen | 38 | Ejercicio Práctico |
| | 39 | Simulacro de examen y corrección |

CSC

CYBER SECURITY CENTRE