Programa Directivo
Ciberseguridad Financiera

El sector financiero está en el **centro de la transformación digital**, pero también es uno de los más expuestos a las **amenazas cibernéticas**. Hoy, la ciberseguridad ya no es solo una cuestión técnica: es un **reto estratégico** que impacta directamente en la continuidad del negocio, la **reputación corporativa** y el cumplimiento normativo.

Nuestro programa en Ciberseguridad Financiera está **diseñado para formar a líderes capaces de gobernar la seguridad digital** desde una perspectiva estratégica. Aprenderás a **anticipar riesgos**, alinear la inversión en ciberseguridad con los objetivos de negocio y **construir organizaciones resilientes** frente a incidentes.

Aspectos destacables y objetivos

- Ofrecer una visión integral, estratégica y práctica de la **seguridad en el entorno financiero**
- Brindar a los participantes una comprensión profunda del **ciberespacio**, las **amenazas emergentes** y su **impacto en el negocio**
- Dotar a los líderes financieros y de riesgo de **herramientas de gestión y gobierno** en materia de ciberseguridad
- Facilitar el **cumplimiento normativo** y la **integración de la ciberseguridad** en el sistema de control interno
- Reforzar la capacidad de **anticipación**, **detección**, **respuesta** y **recuperación** frente a incidentes críticos
- Impulsar una cultura organizacional orientada a la resiliencia y la **protección del valor empresarial**
- Aprender a estructurar una función de **ciberseguridad robusta**, **responder eficazmente a incidentes**, garantizar la continuidad del negocio y cumplir con los marcos regulatorios más exigentes

Modalidad Presencial/Streaming | **Título expedido por IEB**

V de 16-20h | **36h** | **5.500€**

Claustro

Francisco Zea Pasquín
Capitán de Navío y Strategic Account Manager, Oesia/Tecnobit

Andrés Parro
Managing Director, Cybersecurity - Spain
FTI Consulting

Enrique Castañeda de Benito
Teniente Coronel y Jefe de Estudios, EMCO

Fernando Palop Alcaide
Teniente Coronel y Director, Escuela Militar de Ciberoperaciones (EMCO)

Valentín Martín Manzanero
Ingeniero en Ciberseguridad y profesor universitario

Programa

MODULO 1: INTRODUCCIÓN AL CIBERESPACIO Y LA CIBERSEGURIDAD

1.1. CIBERESPACIO Y CIBERSEGURIDAD

1.2. CONCEPTOS FUNDAMENTALES DE CIBERSEGURIDAD

1.3. CIBERCRIMEN Y HACKTIVISMO. PRINCIPALES TIPOS DE ATAQUES

1.4. ACTORES MALICIOSOS Y APTs.

1.5. CIBERSEGURIDAD Y GEOESTRATEGIA

MODULO 2: ESTRUCTURA DE CIBERSEGURIDAD EN LA ORGANIZACIÓN

2.1. PRINCIPALES ROLES

2.2. PROTEGIENDO LA ORGANIZACIÓN

2.3. INTELIGENCIA DE CIBERAMENAZAS

2.4. AUDITORIAS Y PRUEBAS DE PENETRACIÓN

2.5. FORMACIÓN Y CONCIENCIACIÓN

MODULO 3: CUMPLIMIENTO NORMATIVO Y RIESGOS ASOCIADOS

3.1. REGLAMENTO DE RESILIENCIA OPERATIVA DIGITAL (DORA)

3.2. DIRECTIVA EUROPEA DE CIBERSEGURIDAD (NIS2)

3.3. ESQUEMA NACIONAL DE SEGURIDAD (ENS)

3.4. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (GDPR)

3.5. RIESGOS ASOCIADOS A LA FALTA DE CUMPLIMIENTO NORMATIVO

MODULO 4: GESTIÓN DE RIESGO. RIESGO OPERACIONAL

4.1. INTRODUCCIÓN A LA GESTIÓN DE RIESGO

4.2. RIESGO OPERACIONAL

4.3. MODELO DE LAS TRES LÍNEAS DE DEFENSA

4.4. INDICADORES: KPIs y KRIs

4.5. RIESGO EN PROVEEDORES Y ATAQUES A LA CADENA LOGÍSTICA

4.6. AMENAZAS EN EL ENTORNO FINANCIERO Y RIESGOS ASOCIADOS

MODULO 5: CONTINUIDAD DE NEGOCIO Y RESPUESTA A INCIDENTES

5.1. PLANES BCP

5.2. PREVENCIÓN Y RESPUESTA A INCIDENTES. PLANES DRP

5.3. SIMULACROS Y EJERCICIOS

5.4. RESILIENCIA OPERATIVA

5.5. COMITÉ DE CRISIS

MODULO 6: CULTURA ORGANIZACIONAL Y LIDERAZGO

6.1. CULTURA VS CUMPLIMIENTO

6.2. CONCIENCIACIÓN

6.3. GESTIÓN DEL CAMBIO

6.4. LIDERAZGO Y RIESGOS ASOCIADOS

A quién va dirigido

Personal Directivo y con Cargos Intermedios en las áreas Financiera y de Riesgos, Auditoria, Continuidad de Negocio y Seguridad