fundación CAJA INMACULADA

escuela de negocios

JORNADA – Ciberriesgos en la empresa actual: cómo protegerte, responder y asegurarte
Aula virtual

Lugar:	Aula Virtual 976 355 000
Fechas:	**3/6/2026**
Horario:	de 9.30 a 12.30 h.
Importe:	70 €
Importe desempleados:	21 €
Plazo de inscripción: **(Hasta las 15 h.)**	29/5/2026

Presentación

Objetivos

Este curso se centra en los riesgos digitales que amenazan hoy a cualquier organización y en cómo impactan a nivel técnico, operativo, económico y legal.
El enfoque principal es la prevención, los controles de seguridad, la respuesta ante incidentes y los puntos críticos donde suelen fallar las empresas.
El seguro de ciberriesgos se analizará como un elemento más dentro de la estrategia de resiliencia.

Profesorado

D. **Antonio Santos Mayoral.** Responsable Siniestros en Líneas Financieras, Programas Internacionales y Reaseguro en Howden. Especialista en ciberseguridad

Programa

Módulo 1 – El riesgo cibernético como riesgo empresarial

- Por qué el riesgo cibernético es hoy un riesgo estratégico.
- Impacto real en continuidad de negocio, reputación y cumplimiento normativo.
- Errores habituales de gestión que amplifican el impacto de un incidente.

Módulo 2 – Amenazas y vulnerabilidades reales

- Ransomware, phishing, brechas de datos, BEC y ataques a la cadena de suministro.
- Factores humanos: ingeniería social y fallos operativos.
- Sistemas, procesos y tecnologías donde se concentran las vulnerabilidades.
- Consecuencias legales (RGPD, NIS2) y económicas tras un ataque.

Módulo 3 – Medidas de prevención y resiliencia

- Controles mínimos exigidos por normativa y buenas prácticas.
- Gestión adecuada de credenciales, MFA y segmentación.

- Backups robustos, protección endpoint, EDR y SOC.
- Formación de empleados y cultura de seguridad.
- Proceso de respuesta ante incidentes y protocolos internos.

Módulo 4 – El seguro de ciberriesgos desde un enfoque técnico

- Qué cubre y qué no cubre un seguro de ciberriesgos.
- Interacción entre ciberseguridad y aseguradora durante un incidente.
- Cómo evitar problemas en la activación de una póliza:
    - evidencias
    - tiempos de notificación
    - coordinación durante la crisis
- La importancia del forensics, la gestión reputacional y la recuperación técnica.

Módulo 5 – Tendencias del ecosistema de amenazas y del mercado

- Evolución del ransomware: bandas, tácticas y presión regulatoria.
- Requisitos mínimos de ciberseguridad exigidos hoy por aseguradoras (sin enfoque comercial).
- Incremento de ataques a pymes y empresas de servicios.
- Impacto del ransomware-as-a-service y ataques a la cadena de suministro.

Módulo 6 – Casos prácticos y análisis de incidentes

- Análisis de ataques reales y lecciones aprendidas.
- Cómo actuaron las empresas, qué consecuencias tuvieron y cómo se podrían haber mitigado.
- Qué papel jugó (o podría haber jugado) el seguro como apoyo técnico y financiero.

Organización

Plazo de inscripción

La recepción de solicitudes finalizará el 29 de mayo, a las 15,00 horas. Plazas limitadas a la capacidad del aula. **Esta formación no es bonificable**. Se enviará confirmación por correo electrónico. Las cancelaciones efectuadas con posterioridad a dicha fecha, estarán sujetas a la retención del 40% de la cuota de inscripción
Teléfono de información 976 355 000

Cuota de inscripción y forma de pago

- Importe para desempleados (previa confirmación de la plaza) pago con tarjeta de crédito: 21 euros (incluye documentación).
- Importe para pagos por domiciliación o tarjeta de crédito (previa confirmación de la plaza):70 euros (incluye documentación).