icea
El Valor del Conocimiento

Programa Avanzado:

Mejora de la resiliencia Operativa de las compañías: DORA y Gestión de Riesgos

Webinar
Del 17 de marzo al 7 de abril de 2025

METODOLOGÍA

El programa se estructura en 6 sesiones independientes, abarcando diferentes escenarios en los que será de aplicación la normativa DORA.

El alumno puede optar por realizar el **programa completo** o solo aquellas **sesiones individuales** que sean de su interés. Será necesario inscribirse al programa completo o cada una de las sesiones individuales que le interesen.

DIRIGIDO A

Este curso está dirigido a profesionales del sector asegurador con conocimientos básicos del reglamento DORA, así como a aquellos involucrados en la gestión, supervisión, control o auditoría de riesgos tecnológicos y de proveedores TIC. También está orientado a auditores internos, responsables de cumplimiento normativo, gestores de riesgos, y líderes de áreas de tecnología, sistemas y operaciones. Su objetivo es proporcionar las herramientas necesarias para una gestión eficaz de los riesgos emergentes, asegurando el cumplimiento de normativas como DORA y fomentando un enfoque proactivo y anticipatorio en la gestión de estos desafíos.

OBJETIVOS

La nueva normativa DORA exige a las organizaciones del sector financiero fortalecer su resiliencia operativa y la gestión de riesgos TIC. Este curso te brindará un enfoque práctico para cumplir con sus requisitos, abordando la ciberseguridad, la gestión de incidentes, el control de proveedores y la continuidad de negocio. Aprende a implementar un marco de cumplimiento sólido y anticiparte a los desafíos regulatorios, asegurando la estabilidad y seguridad de tu organización en un entorno digital cada vez más exigente

1. Comprender los fundamentos de la ciberseguridad y gestión de riesgos emergentes, incluyendo outsourcing y riesgos TIC.
2. Garantizar el cumplimiento normativo de DORA, incluyendo RTS e ITS, mediante un gap análisis y la identificación de brechas.
3. Implementar un marco efectivo de gestión, clasificación y notificación de incidentes TIC, estableciendo funciones y planes de comunicación.
4. Diseñar estrategias para una gestión eficiente de proveedores y terceros, mitigando riesgos asociados.
5. Fortalecer la cultura de riesgos y seguridad dentro de la organización.
6. Desarrollar planes de continuidad de negocio (BCM) para mejorar la resiliencia operativa ante crisis e incidentes.
7. Construir un plan de acción para la adecuación y cumplimiento progresivo de DORA.

CALENDARIO

- Fechas: 17, 24, 27 y 31 de marzo, 3 y 7 de abril de 2025.
- Carga lectiva:

  Programa completo: 14 horas lectivas.

  Módulos individuales: Sesiones días 17, 24, 27 de marzo, 3 y 7 de abril 2 horas.

  Sesión 31 de marzo 4 horas.

- Horario: 17, 24, 27 de marzo, 3 y 7 de abril de 09:30 h. a 11:30 h.

  31 de marzo de 09:30 h. a 13:30 h.

MARZO

L	M	X	J	V	S	D
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

ABRIL

L	M	X	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

SESIONES

Sesión 1: Riesgos emergentes, gestión de riesgos y control interno

Fecha y horario: 17 de marzo de 09:30 a 11:30 h.

Duración: 2 horas.

Objetivo: Comprender que tipologías de riesgos existen en una compañía considerando riesgos emergentes como los riesgos de outsourcing y de IT en los que se focaliza DORA. Comprender los conceptos básicos y el modelo de gestión de riesgos a establecer en una compañía profundizados en aspectos básicos como el apetito al riesgo y el perfil de riesgo y analizar la relevancia de la cultura transversal de riesgos en la organización y en los roles y responsabilidades del modelo de control interno.

Programa:

- Introducción
- Estándares: ISO 31.000
- Identificación de riesgos y métricas
- Riesgos emergentes (Considerando los requerimientos de DORA)
- Governance, cultura y formación
- Marco de control interno
- Resumen y conclusiones

Sesión 2: Ciberseguridad y modelos operativos resilientes

Fecha y horario: 24 de marzo de 09:30 a 11:30 h.

Duración: 2 horas.

Objetivo: Comprender los fundamentos de la ciberseguridad adquiriendo conocimientos sobre los conceptos básicos de la ciberseguridad, incluyendo las amenazas comunes, los tipos de ataques, medidas de protección y buenas prácticas con el fin de gestionar adecuadamente los Riesgos de IT a los que una compañía está expuesta.

Programa:

- Establecimiento de objetivos y definición de estrategia
- Nuevos modelos de negocio y cómo afrontar la resiliencia
- Regulación y governance
- Análisis de riesgos
- Ciberseguridad, seguridad en sistemas y aplicaciones
- Resumen y conclusiones
- Control y seguimiento del outsourcing
- Resumen y conclusiones

Sesión 3: Gestión outsourcing y normativa DORA

Fecha y horario: 27 de marzo de 09:30 a 11:30 h.

Duración: 2 horas.

Objetivo: En esta sesión se analizará cómo llevar a cabo un proceso de Outsourcing y cómo efectuar la gestión de riesgos derivados del mismo que pueden impactar en la supervivencia del negocio, revisando además lo requerimientos de DORA en cuanto a la gestión de riesgos de terceros.

Programa:

- Introducción
- Análisis de la estrategia de outsourcing
- Requerimientos regulatorios y normativa DORA
- Negociación del outsourcing y toma de decisiones
- Implantación y despliegue del outsourcing
- Control y seguimiento del outsourcing
- Resumen y conclusiones

Sesión 4: GAP análisis y el plan de adecuación a DORA

Fecha y horario: 31 de marzo de 09:30 a 13:30 h.

Duración: 4 horas.

Objetivo: Capacitar a los asistentes en una metodología práctica para evaluar el nivel de cumplimiento de DORA y sus RTS e ITS, identificando brechas a través de un gap análisis y desarrollando un plan de adecuación con acciones proporcionales y efectivas para garantizar la alineación con la normativa.

Programa:

En esta sesión se presentará una metodología de trabajo que capacite a los asistentes para:

- Ejecutar un diagnóstico (gap análisis) del cumplimiento actual de DORA y sus RTS e ITS.
- Elaborar un plan de adecuación que detalle las acciones a implementar a partir de los resultados del gap análisis considerando el principio de proporcionalidad.

Sesión 5: Gestión, clasificación y notificación de incidentes relacionados con las TIC según los requisitos de DORA

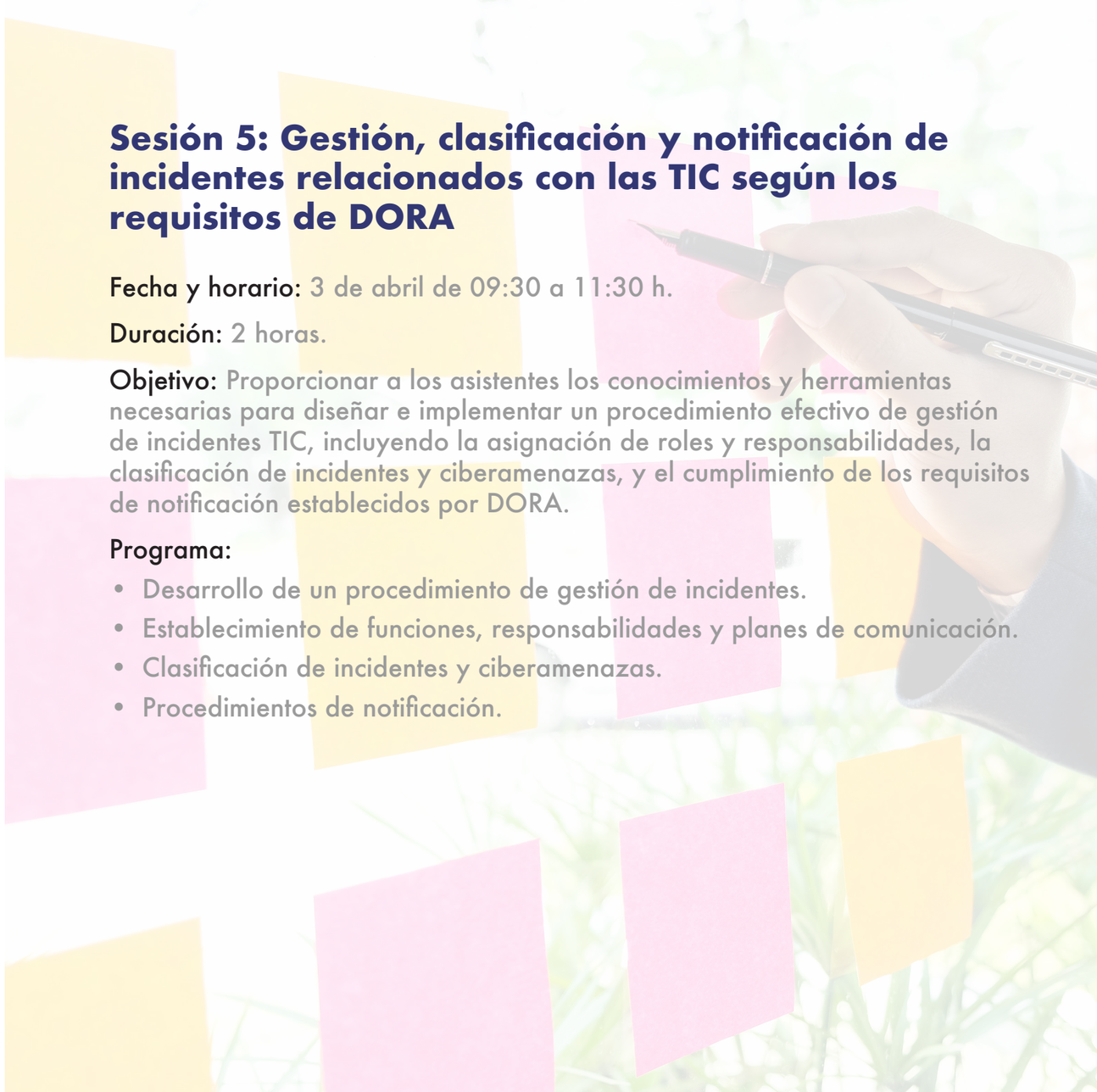
Fecha y horario: 3 de abril de 09:30 a 11:30 h.

Duración: 2 horas.

Objetivo: Proporcionar a los asistentes los conocimientos y herramientas necesarias para diseñar e implementar un procedimiento efectivo de gestión de incidentes TIC, incluyendo la asignación de roles y responsabilidades, la clasificación de incidentes y ciberamenazas, y el cumplimiento de los requisitos de notificación establecidos por DORA.

Programa:

- Desarrollo de un procedimiento de gestión de incidentes.
- Establecimiento de funciones, responsabilidades y planes de comunicación.
- Clasificación de incidentes y ciberamenazas.
- Procedimientos de notificación.



Sesión 6: Continuidad de negocio un paso más en el cumplimiento de DORA

Fecha y horario: 7 de abril de 09:30 a 11:30 h.

Duración: 2 horas.

Objetivo: En aras de mejorar la resiliencia operativa y cumplir con los objetivos establecidos en DORA, la continuidad de negocio juega un papel crucial y diferencial para ser anticipativo. En este curso el participante comprenderá en qué consiste el BCM, Business Continuity Management, como metodología de gestión integral y anticipativa ante posibles futuros incidentes o crisis que puedan poner en peligro la estrategia y la supervivencia del negocio.

Programa:

- Introducción
- Aspectos básicos y análisis de situación
- Normativa y estándares: Requerimientos regulatorios e ISO 22.301
- Amenazas, impacto y soluciones
- Mapa de procesos y fases del BCM: foco en escenarios de pérdida de infraestructura tecnológica
- Resiliencia Operativa
- Conclusiones

PONENTES

Isabel Sánchez

Manuel Mendiola

DATOS DE ORGANIZACIÓN

El alumno podrá inscribirse en el **programa completo** o realizar las inscripciones en los **módulos individuales** que sean de su interés.

Asistencia y Evaluación

Para poder obtener el certificado de superación del curso completo será requisito necesario asistir, como mínimo, al 80% de las clases.

Es de máxima importancia, para el buen aprovechamiento del Programa, la implicación del alumno y la participación en las aulas.

Para obtener el certificado de las sesiones individuales será necesario asistir a la sesión completa.

Admisiones

Desde la apertura de la convocatoria hasta el 14 de marzo de 2025 para el curso completo.

Inscripciones para sesiones individuales hasta la semana anterior a su realización.

Para más información:

Los interesados pueden realizar las consultas que precisen sobre el programa formativo, proceso de admisión y presentación de solicitudes, dirigiéndose a:

Bárbara Sequera
barbara.sequera@icea.es
Tfno. 91 142 09 91

Formación bonificable en Seguros Sociales a través de FUNDAE

Matrícula

Importe de matrícula curso completo

- Entidades Adheridas: 750,40 euros + 21% IVA
- Entidades No Adheridas: 900,50 euros + 21% IVA

Sesiones días 17, 24, 27 de marzo, 3 y 7 de abril de 2025, módulo individual de 2 horas:

- Entidades Adheridas: 213,5 euros + 21% IVA
- Entidades No Adheridas: 277,30 euros + 21% IVA

Sesión 31 de marzo de 2025, módulo individual de 4 horas:

- Entidades Adheridas: 315,80 euros + 21% IVA
- Entidades No Adheridas: 410,50 euros + 21% IVA

Formación bonificable en Seguros Sociales a través de FUNDAE

Condiciones de inscripción:

La cuota de inscripción puede hacerse efectiva mediante transferencia bancaria a nuestra c/c nº: IBAN ES49 0081-7118-57-0001087611 del Banco Sabadell Atlántico de la calle Juan Bravo, 51 (28006 Madrid).

icea
El Valor del Conocimiento

ICEA
López de Hoyos, 35 - 5ª planta. 28002 Madrid
Tel: 91 142 09 00
www.icea.es
@icea_es
Asociación ICEA