WORLD COMPLIANCE ASSOCIATION *Evento Recomendado*



PRESENCIAL

La Nueva Frontera del Compliance: Riesgos Digitales y Ciberseguridad

DESCRIPCIÓN DEL EVENTO

La digitalización ha reconfigurado la forma en que operan las organizaciones, pero también ha ampliado la superficie de riesgo. Hoy, la integridad empresarial depende tanto de los controles tradicionales como de la capacidad para enfrentar ciberamenazas, proteger datos y prevenir abusos tecnológicos.

Este evento profundiza en la convergencia entre compliance y ciberseguridad y ofrece herramientas prácticas para anticipar, detectar y responder a los riesgos digitales que definirán las prioridades de las organizaciones en 2026.

FECHA DEL EVENTO
2026-03-26

LUGAR

HORARIO
08:30 - 10:30

PRECIO
50 USD
Precio para asociados: 35 USD

INFORMACIÓN ADICIONAL

Inscríbete al Evento

WORLD COMPLIANCE ASSOCIATION *Evento Recomendado*



PRESENCIAL

La Nueva Frontera del Compliance: Riesgos Digitales y Ciberseguridad

OBJETIVOS

Fortalecer las capacidades de líderes y profesionales para identificar, gestionar y mitigar riesgos digitales y ciberamenazas, integrando prácticas de compliance, gobernanza de datos y ciberseguridad desde una perspectiva estratégica y operativa.

PROGRAMA

Módulo 1 — Panorama Actual del Riesgo Digital (2025–2026)

- Tendencias y evolución de ciberamenazas en la región.
- Inteligencia artificial: riesgo emergente y herramienta defensiva.
- Marco normativo clave: protección de datos, ciberseguridad y compliance digital.
- Responsabilidad de la Alta Dirección y Juntas Directivas en la gobernanza tecnológica.

Módulo 2 — Compliance Digital y Controles en Entornos Tecnológicos

- Fraude, corrupción y soborno en ecosistemas digitales.
- Due diligence tecnológica y evaluación de proveedores críticos.
- Controles internos para entornos cloud, automatización y plataformas digitales.
- Indicadores esenciales para monitorear riesgos digitales.

Módulo 3 — Ciberseguridad Aplicada al Compliance

- Diseño de un Programa de Cibercompliance.
- Gestión y respuesta a incidentes (protocolos, comunicación y documentación).
- Evidencia digital y su rol en las investigaciones internas.
- Reputación y obligaciones en casos de brechas de datos.

Módulo 4 — Taller Práctico: Simulación de un Ciberataque

Un ejercicio dinámico que integra a todas las áreas:

- Línea de tiempo del incidente.
- Acciones del área de TI, Compliance y Relaciones Corporativas.
- Decisiones clave de la Alta Dirección.
- Errores comunes, aprendizajes y checklist final para implementar mejoras inmediatas.

DIRIGIDO A

Alta Dirección

- CEO, CFO, COO
- Presidentes y miembros de Junta Directiva

Áreas de Cumplimiento y Riesgo

- Oficiales de cumplimiento
- Gerentes de riesgo
- Auditores internos

Áreas Técnicas

- CIO / CTO
- Equipos de TI y ciberseguridad
- Analistas de datos

Sectores clave

- Bancario y financiero
- Telecomunicaciones
- Retail
- Gobierno y sector público

Empresas certificadas o interesadas en certificaciones ISO (37001, 27001, 37301, etc.)