Curso
Ciberseguridad y Ciber Riesgos para el Sistema Financiero Mexicano

Objetivo General:

Fortalecer las capacidades de los participantes para comprender, evaluar y gestionar los riesgos de ciberseguridad y ciber resiliencia en instituciones financieras mexicanas, integrando los principios de resiliencia operativa digital. Al finalizar, los asistentes podrán diseñar estrategias, controles y modelos de gobernanza que incrementen la seguridad, la continuidad operativa y la confianza del cliente.

Dirigido a:

•CISOs, CROs y responsables de Seguridad de la Información.

•Directores y gerentes de TI, Riesgos Tecnológicos y Continuidad de Negocio.

•Equipos de Ciberseguridad, SOC, Red Team, Blue Team y Respuesta a Incidentes.

•Oficiales de Cumplimiento, Auditoría Interna y áreas regulatorias.

•Fintech, SOFIPOs, SOFOMES, casas de bolsa y entidades supervisadas por CNBV, Banxico y CONDUSEF.

•Profesionales que participan en proyectos de transformación digital, nube, IA y automatización.

Objetivos Específicos:

Al finalizar el curso, los participantes podrán:

•Comprender el marco de resiliencia operativa digital y su relevancia para el sistema financiero mexicano.

•Identificar y evaluar riesgos tecnológicos, ciber riesgos y dependencias críticas.

•Alinear prácticas internas con los principios internacionales (P. Ej., DORA, NIS2, etc.) y la regulación mexicana vigente.

•Diseñar estrategias de ciberseguridad basadas en riesgo, continuidad y gobernanza.

•Implementar modelos de gestión de incidentes, pruebas de resiliencia y supervisión de terceros.

•Reconocer tendencias emergentes (IA, agentes, cloud, supply chain) y su impacto en la ciberseguridad financiera.

Temario

Módulo 1 — Ciberseguridad en el Sistema Financiero: Evolución, Contexto y Tendencias

Ponente: Julián Zamora

•Transformación digital del sector financiero y nuevas superficies de ataque.

•Lecciones recientes: incidentes globales, disrupciones operativas y riesgos sistémicos.

•Principios de resiliencia operativa digital.

•Impacto de IA, automatización, nube y agentes en la ciberseguridad.

•Expectativas actuales de clientes, reguladores y mercados.

Duración: 2 horas

Módulo 2 — Gestión de Riesgos Tecnológicos y Ciber Riesgos

Ponente: Geraldine Ariza

•Marcos de Gestión En Riesgos.

•Definición, clasificación y taxonomía de riesgos tecnológicos y ciber riesgos.

•Modelos de gestión basados en riesgo: identificación, evaluación, mitigación y monitoreo.

•Riesgos emergentes

•Integración con GRC, continuidad de negocio y gobierno corporativo.

•Tres líneas de Defensa

•Caso práctico: evaluación de un riesgo tecnológico crítico.

•Actividad practica: Identificación de riesgos, activos y control.

Duración: 2 horas

Módulo 3 — Ciber Riesgos en el Sector Financiero: Amenazas, Modus Operandi y Controles

Ponente: Julián Zamora

•Amenazas actuales: ransomware, fraude digital, phishing avanzado, ataques a APIs, deepfakes, IA ofensiva.

•Modus operandi de atacantes en banca, fintech y mercados.

•Controles críticos: Zero Trust, MFA, segmentación, monitoreo, hardening, detección y respuesta.

•Gestión de incidentes: preparación, contención, erradicación, recuperación y comunicación.

•Lecciones aprendidas de incidentes reales.

Duración: 2 horas

Módulo 4 — El Sistema Financiero Mexicano y su Marco Regulatorio

Ponente: Julián Zamora

•Estructura del sistema financiero: sectores, participantes y funciones.

•Rol de CNBV, Banxico, CONDUSEF, IPAB y otras autoridades.

•Obligaciones actuales en ciberseguridad-

•Convergencia con estándares globales: ISO 27001, NIST CSF, NIST 800-53, PCI DSS.

•Cómo se compara México con DORA y NIS2.

Duración: 2 horas

Módulo 5 — DORA como Referencia Internacional para México

Ponente: Julián Zamora

•Qué es DORA y por qué es relevante para instituciones mexicanas.

•Cinco pilares de DORA:

1. Gestión de riesgos TIC
2. Gestión de incidentes y reporte
3. Pruebas de resiliencia digital
4. Gestión de terceros críticos
5. Intercambio de información

•Lecciones aplicables al contexto mexicano.

•Cómo alinear una institución mexicana para estándares tipo DORA.

Duración: 2 horas

Módulo 6 — Futuro de la Regulación y la Resiliencia Operativa en México

Ponente: Julián Zamora

•Tendencias regulatorias globales: DORA, NIS2, FFIEC, MAS, FCA.

•Hacia dónde se mueve México: expectativas de CNBV y Banxico.

•Gobernanza, métricas y KPIs de resiliencia operativa.

•Preparación institucional: cultura, talento, procesos y tecnología.

•Conclusiones y recomendaciones estratégicas para los próximos 24 meses.

Duración: **2** horas

Duración total: **12 horas**

Ing. Geraldine Ariza Miñoz

Profesional en gestión de riesgos con experiencia acompañando a organizaciones en el diseño, implementación y fortalecimiento de sus sistemas de control, calidad y continuidad.

A lo largo de su trayectoria, ha aprendido que la gestión de riesgos no se trata únicamente de metodologías o marcos normativos, sino de generar confianza: de anticipar escenarios, tomar decisiones informadas y ayudar a que las organizaciones operen con mayor claridad y resiliencia.

Es Ingeniera Industrial, especialista en Gestión de Riesgos y Seguros, con formación en estándares internacionales como ISO 9001, ISO 14001, ISO 27001 y marcos como ISO 31000 y COSO. Ha participado en la estructuración de sistemas integrados de gestión, la definición de indicadores, la gestión de riesgos operativos (SARO) y de cumplimiento (SARLAFT), así como en procesos de auditoría y mejora continua.

Actualmente se desempeña como Customer Success Specialist, donde acompaña a organizaciones a nivel global en la adopción y madurez de sus prácticas de gestión de riesgos. Su rol integra capacidades técnicas y de negocio, permitiéndole traducir conceptos complejos en soluciones prácticas, así como fortalecer la cultura de riesgos a través de capacitaciones, workshops y espacios de aprendizaje.

Cree en una gestión de riesgos cercana al negocio: aquella que no solo cumple con estándares, sino que habilita decisiones, impulsa la mejora continua y genera valor sostenible en las organizaciones.

Mtro. Luis Julián Zamora Ábrego

Profesional con más de 25 años liderando la intersección entre negocio, tecnología y personas, con un enfoque estratégico en ciberseguridad, resiliencia operativa y gestión de riesgos.

A lo largo de su carrera, ha acompañado a organizaciones a fortalecer su capacidad de anticipar, resistir y recuperarse ante eventos críticos, entendiendo que la resiliencia no es solo un tema tecnológico, sino un habilitador de confianza, continuidad y sostenibilidad del negocio.

Es Ingeniero en Electrónica y Comunicaciones por la Universidad Iberoamericana y cuenta con un MBA por el ITAM. Con varias certificaciones en seguridad, riesgo y gestión de tecnología. Su trayectoria le ha llevado por organizaciones como BBVA, CyberInt Inc., la Bolsa Institucional de Valores (BIVA), Atos Global Delivery Center y PMI Comercio Internacional, donde ha liderado equipos multidisciplinarios y diseñado estrategias para fortalecer la gobernanza tecnológica, la gestión integral de riesgos y la continuidad del negocio.

Paralelamente, ha cultivado una sólida carrera académica, convencido de que compartir conocimiento transforma realidades. Ha tenido la oportunidad de acompañar a nuevas generaciones de profesionales en el camino de la ciberseguridad y la innovación.

Cree profundamente en el poder de la tecnología bien gobernada: aquella que protege lo esencial, impulsa la colaboración y permite que las organizaciones sigan avanzando sin perder su propósito.

Informes e inscripciones:

info@cbfgloval.com.mx

Teléfonos: 55 55 46 26 60
442 340 90 56

Whatsapp: 442 330 60 05