



CURSO ONLINE

➤ ***Gestión de Riesgo Tecnológico en Bancos e Instituciones Financieras***

5 de mayo al 2 de junio de 2026



INFORMACIÓN GENERAL

PRESENTACIÓN

En la actualidad, los bancos e instituciones financieras dependen de la tecnología para operar de manera eficiente y segura. Sin embargo, esta dependencia también aumenta la exposición a riesgos tecnológicos que pueden afectar la continuidad de las operaciones, la seguridad de la información, el cumplimiento regulatorio y la reputación institucional.

Conscientes de la importancia para las instituciones financieras el riesgo tecnológico que enfrentan, ALIDE presenta su Curso Online sobre **Gestión de Riesgo Tecnológico en Bancos e Instituciones Financieras**, con la finalidad de capacitar a profesionales del sector financiero en la identificación, evaluación, mitigación y control del riesgo tecnológico, alineando la estrategia tecnológica con las necesidades del negocio y los requisitos regulatorios. A través de un enfoque práctico y basado en casos reales, los participantes aprenderán a fortalecer la resiliencia operativa, la ciberseguridad y la continuidad del negocio de sus organizaciones.

DURACIÓN DEL CURSO

Se desarrollará en 5 sesiones teniendo un total de 15 horas lectivas, con la atención personalizada del expositor y el acceso al Campus Virtual de ALIDE, www.alidevirtual.org. Se utilizará la plataforma de videoconferencia "Zoom", por lo que podrán acceder a las sesiones desde una computadora personal o de escritorio, celulares y tabletas.

FECHAS

Se realizará de acuerdo con las fechas y horarios siguientes:

Sesión	Fechas	Horas	Horario *	Módulos
1	Martes, 5 de mayo	3	3:00 a 6:00 pm	Módulo I: Introducción al Riesgo Tecnológico y su Contexto en el Sector Financiero
2	Martes, 12 de mayo	3	3:00 a 6:00 pm	Módulo II: Identificación y Evaluación de Riesgos Tecnológicos
3	Martes, 19 de mayo	3	3:00 a 6:00 pm	Módulo III: Marco de Gestión, Gobierno y Buenas Prácticas Internacionales
4	Martes, 26 de mayo	3	3:00 a 6:00 pm	Módulo IV: Mitigación y Control del Riesgo Tecnológico
5	Martes, 2 de junio	3	3:00 a 6:00 pm	Módulo V: Casos Prácticos, Simulaciones y Plan de Gestión

* Hora de Perú. Para visualizar tu hora local, hacer [clic aquí](#) y digita tu ciudad en el campo "Agregar otra ciudad"

OBJETIVOS

Al participar en este curso, los asistentes obtendrán:

1. Comprensión profunda de los principales riesgos tecnológicos que enfrentan los bancos y otras instituciones financieras.
2. Habilidad para evaluar impactos en operaciones, clientes, cumplimiento y reputación.
3. Conocimiento de marcos y buenas prácticas internacionales de gestión de riesgos y ciberseguridad.
4. Capacidad para integrar la gestión de riesgo tecnológico con riesgos operativos, de ciberseguridad y continuidad de negocio.
5. Experiencia práctica mediante ejercicios, simulaciones y desarrollo de planes de mitigación y control de riesgos tecnológicos.
6. Herramientas para fortalecer la resiliencia operativa y la seguridad de la información en sus organizaciones.

OBJETIVOS ESPECIFICOS

- ✓ Comprender los principales tipos de riesgo tecnológico en el sector financiero y su impacto en la organización.
- ✓ Identificar riesgos asociados a infraestructura, software, datos, terceros y nube.
- ✓ Evaluar impactos de los riesgos tecnológicos sobre operaciones, clientes, cumplimiento normativo y reputación institucional.
- ✓ Aplicar marcos internacionales y buenas prácticas para la gestión de riesgos tecnológicos y ciberseguridad.
- ✓ Integrar la gestión del riesgo tecnológico con los riesgos operacionales, de ciberseguridad y continuidad de negocio.
- ✓ Diseñar un plan básico de gestión y control del riesgo tecnológico adaptado a la realidad de su institución.

PROGRAMA TEMÁTICO

Módulo I: Introducción al Riesgo Tecnológico y su Contexto en el Sector Financiero No. de horas: 3

Objetivos:

- Comprender el concepto de riesgo tecnológico y su relevancia en el sector financiero.
- Conocer el impacto de la tecnología en operaciones, clientes, reputación y cumplimiento.
- Diferenciar riesgo tecnológico, riesgo operacional y riesgo de ciberseguridad.

Temas:

1. Evolución de la tecnología en el sector financiero.
2. Principales tipos de riesgo tecnológico (infraestructura, software, datos, terceros, nube).
3. Normativas y regulación aplicables.
4. Relación entre riesgo tecnológico, operacional, ciberseguridad y continuidad del negocio.

Módulo II: Identificación y Evaluación de Riesgos Tecnológicos No. de horas: 3

Objetivos:

- Identificar riesgos tecnológicos relevantes en la organización.
- Evaluar su impacto y probabilidad, priorizando los riesgos críticos.

Temas:

1. Riesgos asociados a infraestructura, software, datos, terceros y nube.
2. Métodos de identificación de riesgos: cuestionarios, entrevistas, análisis de incidentes.
3. Evaluación del impacto en operaciones, clientes, cumplimiento y reputación.
4. Herramientas y métricas de evaluación de riesgo tecnológico.

Módulo III: Marco de Gestión, Gobierno y Buenas Prácticas Internacionales No. de horas: 3
--

Objetivos:

- Conocer marcos internacionales para gestionar el riesgo tecnológico.
- Aplicar buenas prácticas para fortalecer la resiliencia y la seguridad.

Temas:

1. ISO 31000: gestión de riesgo.
2. ISO 27001: seguridad de la información.
3. NIST Cybersecurity Framework.
4. COBIT 2019 y control de TI.
5. Integración con planes de continuidad de negocio y ciber resiliencia.

Módulo IV: Mitigación y Control del Riesgo Tecnológico No. de horas: 3

Objetivos:

- Diseñar e implementar controles para reducir el riesgo tecnológico.
- Aplicar estrategias de mitigación y monitoreo continuo.

Temas:

1. Controles tecnológicos: acceso, cifrado, respaldo y recuperación.
2. Gestión de proveedores y riesgos de terceros.
3. Evaluación de ciberseguridad y pruebas de penetración.
4. Planes de respuesta ante incidentes y continuidad de negocio.
5. Integración de controles con auditoría interna y cumplimiento regulatorio.

Objetivos:

- Aplicar los conocimientos adquiridos en escenarios prácticos.
- Elaborar un plan básico de gestión del riesgo tecnológico para su institución.

Temas:

1. Evaluación de impactos y priorización de acciones correctivas.
2. Desarrollo de un plan de gestión y control del riesgo tecnológico.
3. Integración de riesgo tecnológico con riesgos operacionales, de ciberseguridad y continuidad.
4. Casos recientes de explotación de riesgos tecnológicos y sus lecciones.
5. Diversos tipos de ciber-ataques

ENFOQUE METODOLÓGICO

Nuestro modelo de formación se basa en una acción tutorial constante, en donde el participante estudiará de acuerdo con su tiempo y disponibilidad.

Cabe resaltar que en el Campus Virtual de ALIDE se colocará el enlace para las videoconferencias que se tendrán en cada una de las sesiones, a través de la plataforma “Zoom”, por lo que podrán acceder a las sesiones desde una computadora personal o de escritorio, celulares y tabletas. Cabe mencionar que, si el participante no pudiese de participar en alguna sesión, le brindaremos la grabación de esta, la cual será publicada en el campus virtual de ALIDE.

Los participantes contarán con el acompañamiento permanente del expositor, a quien se le puede formular las preguntas y dudas que se tenga para recibir las orientaciones y respuestas a las consultas individual o grupalmente. Ello puede ser así en el desarrollo de las sesiones o a través de la opción de comunicación con el expositor que tiene el campus virtual de ALIDE.

PARTICIPANTES

Gerentes, jefes de área de TI, Riesgos, Seguridad, Continuidad y Cumplimiento en bancos comerciales, bancos de desarrollo, instituciones financieras no bancarias, organismos de supervisión bancaria y además de todos aquellos profesionales relacionados en el área de riesgos, auditoría de sistemas o auditores en general que requieran tener un conocimiento teórico y práctico sobre la gestión de riesgos.

EXPOSITOR



FRANO CAPETA MONDOÑEDO

Peruano. Ingeniero de Computación y Sistemas, estudios de Postgrado en Tecnologías de Información. Maestría en Administración de Empresas, Especializado en seguridad de la información y continuidad de negocios.

Auditor ISMS (Information Security Management Systems) acreditado por IRCA (International Register Certified Auditors), Auditor BCMS (Business Continuity Management Systems) acreditado por IRCA,

posee las Certificaciones en gobierno empresarial de TI; Certificado CGEIT (Certified in the Governance of Enterprise IT) por ISACA, en riesgos; Certificado CRISC (Certified in Risk and Information Systems Control) por ISACA, Certificado CISO (Chief Information Security Officer) por EC-Council, Certificado en ISO 27002 Information Security Foundations, Certificado en Ciberseguridad como Lead Cybersecurity manager, profesional certificado en Blockchain (CBP – Certified Blockchain Profesional) Certificado como ITIL Expert, con experiencia en implementación y administración de Proyectos de Tecnología de Información, seguridad de la información y continuidad del negocio. Miembro asociado del BCI (Business Continuity Institute), Miembro activo del Colegio de Ingenieros del Perú, miembro activo de ISACA (Information Systems audit and Control Association).

INVERSIÓN Y FORMA DE PAGO

- US\$580 por participante (Institución miembro de ALIDE)
- US\$795 por participante (Institución no miembro de ALIDE)

DESCUENTO CORPORATIVO POR GRUPOS

3% de la cuota correspondiente de 3 hasta 5 participantes
5% de la cuota correspondiente de 6 a más participantes

El importe de las inscripciones es neto sin afectar deducciones, impuestos y retenciones propios del país de procedencia del participante. Por lo tanto, si se va a aplicar deducciones o impuestos al importe neto de la inscripción, debe comunicarse el porcentaje a aplicar, con el fin de emitir la factura por un monto tal que permita cobrar la cuota de inscripción estipulada. No se aplican los descuentos corporativos por grupos en caso se cargue algún impuesto local.

Para efectuar el pago, se debe realizar por intermedio de:

- **Para instituciones en el Perú:**
Depósito bancario a Cta. Cte. N° 193-1132251188 del Banco de Crédito del Perú
- **Para instituciones de otros países:**
Transferencia bancaria a la cuenta corriente de ALIDE N° 75022011-3 del Banco do Brasil S.A. (New York). Dirección: 535 Madison Avenue – 33th floor, New York NY 10022, U.S.A., Teléfono: (1-646) 845-3700 / 845-3752. ABA: 026003557. SWIFT: BRASUS33

Nota: Para todos los países, inclusive Perú, los pagos pueden realizarse mediante tarjeta de crédito (Visa/MC/AMEX/Diners), coordinando previamente con ALIDE.

CERTIFICACIÓN

Se otorgará Certificación Internacional a las personas que completen satisfactoriamente el curso, es decir, que cumplan con lo encomendado por el expositor, de modo tal de obtener un puntaje superior a 7.4 sobre 10 puntos y la participación en cada una de las sesiones ya que también es calificada, por lo que se solicita la activa participación en cada una de ellas. En el certificado se indicará el desempeño obtenido por el participante. Éste será enviado por correo electrónico.

INSCRIPCIONES

El proceso de inscripción se realiza a través del Campus Virtual de ALIDE, www.alidevirtual.org, en el cual existe la opción correspondiente de [REGISTRARSE](#), donde completará un formulario en línea, luego de lo cual se le facilita la confirmación y los pasos para el ingreso al Campus Virtual de ALIDE. **El cierre de inscripción y matrícula del curso vence el martes, 28 de abril de 2026.**

INFORMES Y CONSULTAS

Sr. Sandro Suito

Especialista E-learning

Programa de Fortalecimiento de Capacidades

Sra. Milagros Angulo

Asistente

Programa de Fortalecimiento de Capacidades

E-mail: mangulo@alide.org

ASOCIACIÓN LATINOAMERICANA DE INSTITUCIONES FINANCIERAS PARA EL DESARROLLO (ALIDE)

Paseo de la República 3211, San Isidro, Lima 15047, Perú

Web: www.alide.org