Capacita
e-Learning

Executive Internal Audit Program

GRC y Cyber Risk: Gobierno Estratégico con COBIT 2019, COSO y NIST CSF 2.0.

24, 25, 26 y 27 de marzo, 2026
15:00 Centroamérica
Programa online en vivo

Wilson Andia Cuiza

MSc, CISA, CRISC, CSX, CDPSE, ISO 27001 LA

Descripción del Curso

Introducción

Vivimos en un contexto donde la transformación digital avanza a gran velocidad y la tecnología se ha vuelto esencial para el funcionamiento de las organizaciones. Al mismo tiempo, las amenazas cibernéticas no dejan de crecer y evolucionar. Este escenario hace que los riesgos tecnológicos y de ciberseguridad ya no sean solo un problema técnico, sino un factor que impacta directamente la estrategia, la continuidad del negocio y la reputación de las organizaciones.

El Gobierno, Riesgo y Cumplimiento (GRC) se consolida como un enfoque integral para asegurar que la tecnología y la ciberseguridad estén alineadas con los objetivos estratégicos del negocio, que los riesgos sean gestionados dentro del apetito definido por la Alta Dirección y que se cumpla con regulaciones, estándares y buenas prácticas internacionales.

Este curso integra tres marcos clave y complementarios: COBIT 2019, como marco de Gobierno y Gestión de TI orientado al valor, COSO ERM, como base para la gestión integral de riesgos empresariales. NIST Cybersecurity Framework 2.0, como referencia actualizada para la gestión del riesgo cibernético.

La combinación de estos marcos permite a ejecutivos, responsables de TI, ciberseguridad, riesgos y auditoría comprender cómo establecer un Gobierno Estratégico del Riesgo Cibernético, con un enfoque práctico, alineado al negocio y defendible ante auditorías y reguladores.

Objetivo

Proporcionar a los participantes los conocimientos conceptuales y prácticos necesarios para diseñar, evaluar y fortalecer modelos de Gobierno, Riesgo y Cumplimiento (GRC) enfocados en ciberseguridad y riesgos tecnológicos, aplicables a Entidades Financieras, Empresas Privadas y Organizaciones del Sector Público, integrando los marcos COBIT 2019, COSO ERM y NIST Cybersecurity Framework 2.0, de forma alineada con la estrategia institucional, los objetivos del negocio, las expectativas de la Alta Dirección y los requerimientos regulatorios.

Objetivo específico

- Comprender el rol del Gobierno Corporativo y del Gobierno de TI en la gestión del riesgo cibernético, considerando las exigencias regulatorias y de supervisión propias de Entidades Financieras, así como las necesidades de control y transparencia de Empresas Privadas y Organizaciones del Sector Público.
- Diferenciar claramente entre gobierno, gestión, riesgo, cumplimiento y ciberseguridad, adoptando una visión estratégica orientada al negocio y al interés público, según el tipo de organización.
- Aplicar los principios clave de COBIT 2019 para establecer y evaluar esquemas de gobierno y gestión de TI que generen valor, optimicen riesgos y aseguren el cumplimiento normativo en organizaciones financieras, privadas y públicas.
- Integrar COSO ERM como marco base para la gestión integral del riesgo tecnológico y cibernético, alineando dichos riesgos con la estrategia institucional, el apetito al riesgo y los objetivos organizacionales.
- Comprender la estructura, los principales cambios y el enfoque basado en riesgo de NIST Cybersecurity Framework 2.0, y su aplicación práctica en entornos regulados y no regulados.
- Mapear y alinear COBIT 2019, COSO ERM y NIST CSF 2.0 en un modelo GRC coherente, escalable y defendible ante entes reguladores, auditorías y órganos de control.
- Identificar y definir roles, responsabilidades, líneas de defensa y métricas clave, que faciliten la toma de decisiones ejecutivas y el reporte efectivo a la Alta Dirección, Comités y Consejos.
- Reconocer el enfoque, alcance y expectativas de la Auditoría Interna y Externa en evaluaciones de GRC y Cyber Risk, así como las principales evidencias y criterios de madurez requeridos en Entidades Financieras, Empresas Privadas y Organizaciones Públicas.

¿Porque Asistir?

- Porque el riesgo cibernético ya es un riesgo estratégico, no solo técnico.
- Porque la Alta Dirección y los Consejos demandan información clara, medible y alineada al negocio.
- Porque COBIT, COSO y NIST son marcos complementarios, pero pocas organizaciones saben integrarlos correctamente.
- Porque permite hablar un lenguaje común entre negocio, TI, ciberseguridad, riesgos y auditoría.
- Porque fortalece la capacidad de respuesta ante auditorías, reguladores y eventos de ciberseguridad.
- Porque proporciona una visión práctica, aplicada y orientada a la toma de decisiones.

Metodología

Este seminario de 8 horas se desarrollará en formato online en vivo, dividido en 4 sesiones de 2 horas cada una, permitiendo una interacción directa entre los participantes y el facilitador. La metodología combina la exposición conceptual con ejercicios prácticos, aplicando los lineamientos establecidos en COBIT, COSO y el NIST Cybersecurity Framework 2.0.

Las principales características metodológicas incluyen:

- Clases en tiempo real mediante plataforma virtual, con espacios para consultas, análisis conjunto de textos y discusión de observaciones reales.
- Talleres prácticos de diseño, evaluación y fortalecimiento de modelos de Gobierno, Riesgo y Cumplimiento (GRC) enfocados en ciberseguridad y riesgos tecnológicos, aplicables a Entidades Financieras, Empresas Privadas y Organizaciones del Sector Público.

Descripción del Curso

- Aplicación de COBIT 2019, COSO y NIST 2.0, enfocados en ciberseguridad y riesgos tecnológicos.
- Dinámicas de revisión cruzada entre participantes, fomentando el pensamiento crítico y el aprendizaje colaborativo entre profesionales de distintas industrias.
- Acceso a recursos complementarios digitales, como COBIT 2019, COSO y el NIST Cybersecurity Framework 2.0.

Dirigido a:

- Miembros del Consejo
- Miembros de Comités (ej. de Riesgo y Cumplimiento, Auditoría, de Ciberseguridad y de TI)
- Tecnologías de la información
- Seguridad Cibernética y de la información
- Riesgo Operativo (Riesgo Tecnológico)
- Cumplimiento
- Auditores Internos y Auditores Externos

Contenido

Fundamentos de GRC y gobierno del riesgo cibernético

- Contexto actual del riesgo tecnológico y cibernético
  - Transformación digital y dependencia tecnológica
  - Tendencias de ciberamenazas y su impacto en el negocio
  - Casos reales y lecciones aprendidas
- Conceptos clave de GRC
  - Gobierno vs Gestión
  - Riesgo vs Cumplimiento
  - GRC como habilitador estratégico
- Gobierno Corporativo y Gobierno de TI
  - Rol del Consejo y la Alta Dirección
  - Toma de decisiones basada en riesgo
  - Apetito y tolerancia al riesgo
- Introducción a los marcos de referencia
  - Visión general de COBIT 2019
  - Visión general de COSO ERM
  - Visión general de NIST CSF 2.0

COBIT 2019 como marco de gobierno y gestión de TI

- Principios y componentes de COBIT 2019
  - Sistema de gobierno
  - Componentes del sistema de gobierno
  - Factores de diseño
- Objetivos de Gobierno y Gestión
  - Dominios EDM, APO, BAI, DSS y MEA - Enfoque en creación de valor y optimización de riesgos
- COBIT y la gestión del riesgo
  - EDM03 – Asegurar la Optimización del Riesgo - APO12 – Gestionar el Riesgo - Relación con ciberseguridad
- Métricas y desempeño en COBIT
  - Metas empresariales y metas de alineación - Indicadores y tableros ejecutivos

COSO ERM y NIST CSF 2.0 aplicados al Cyber Risk

- COSO ERM – Enfoque y componentes
  - Gobierno y cultura
  - Estrategia y establecimiento de objetivos
  - Desempeño del riesgo
  - Revisión e información
- Riesgo tecnológico y cibernético
  - Integración del cyber risk en el ERM
  - Eventos, impactos y respuestas al riesgo
- NIST Cybersecurity Framework 2.0
  - Funciones del CSF 2.0
  - Perfil actual vs perfil objetivo
  - Outcomes
- Gestión del riesgo cibernético con NIST
  - Identificación, evaluación y tratamiento del riesgo
  - Relación con controles y madurez

Integración, auditoría y modelo práctico de GRC

- Integración COBIT – COSO – NIST
  - Cómo se complementan los marcos
  - Mapeo de gobierno, riesgo y controles
- Modelo práctico de GRC y Cyber Risk
  - Arquitectura de gobierno
  - Roles y responsabilidades (RACI)
  - Flujos de información ejecutiva
- Enfoque de Auditoría Interna y Externa
  - Qué evalúa Auditoría en GRC y Cyber Risk
  - Evidencias, madurez y cumplimiento
  - Errores comunes y buenas prácticas
- Cierre y conclusiones
  - Mensajes clave para ejecutivos
  - Recomendaciones para implementación progresiva

Wilson Andia Cuiza

CISA, CRISC, CSX, CDPSE, ISO 27001 LA

Tiene en su "ADN" Tecnología y Auditoría, con más de 23 años de experiencia en Auditorías de TI, Seguridad, Riesgos y Control de TI, reconocido en diferentes Bancos como Auditor Externo y por sus conferencias internacionales, así como por las docencias en Certificaciones mundialmente reconocidas y Maestrías de alto impacto.

Wilson es Ingeniero de Sistemas con Postgrados en Seguridad y Auditoría de TI y Certificaciones Internacionales CISA, CRISC, CSX y CDPSE de ISACA e ISO 27001 y es Instructor acreditado CISA y CRISC por APMG. Inicialmente fue Analista Programador en diferentes Empresas. Posteriormente trabajó como Consultor Internacional en Auditoría de TI y Seguridad en países de Sud, Centro América y el Caribe en Bancos de prestigio y Empresas, así como Entidades Fiscalizadoras como Contralorías, Cámara de Cuentas y Tribunal de Cuentas, Proyectos Financiados por BID, Banco Mundial, PNUD y Unión Europea.

Actualmente es Director de Auditorías y Consultorías de TI de una de las Firmas con mayor presencia en República Dominicana en el Sector Bancario, teniendo entre otros clientes a 10 Bancos de prestigio.

El Sr. Andia es experto en:

- Dirección de Auditorías de TI y de Ciberseguridad.
- Auditoría de TI y Seguridad en Bancos Múltiples y de Ahorro y Crédito.
- Auditoría y Seguridad de Core Bancarios: FISERV, FISA, BANCA 2000, SYSDE BANCA, ABANKS.
- Auditoria a Sistemas MONITOR PLUS, SENTINEL CUMPLIMIENTO/PREVENTION, ULTRAFISGON.
- Auditor de TI en Prevención del Lavado de Activos (PLA/FT).
- Auditoría de cumplimiento PCI-DSS.
- Seguridad, Riesgos y Auditoría de TI basado en metodologías y estándares ISO de TI COBIT, COSO, ISO 27001, 27002, 22301, 27031, 12207, 25000, 9126, 15504.
- Desarrollo e Implementación de Planes de Continuidad (BCP) y de Recuperación ante Desastres Informáticos (DRP).
- Desarrollo e Implementación de Políticas de Seguridad de TI.
- Detección de fraudes o delitos informáticos.
- Análisis Forense Informático usando Software (EnCase y Forensic ToolKit, Autopsy)
- Software de Auditoría (IDEA, ACL, TEAM MATE, MEYCOR COBIT, COBIT ADVISOR)
- Ley Sarbanes Oxley (SOX) relacionado con TI.
- Análisis, Programación e Implementación de Sistemas Informáticos.
- Administración de Bases de Datos ORACLE, SQL SERVER, SYSBASE, DB2.
- Lenguajes de programación ORACLE, .NET. C#, Java.
- Conferencias Internacionales de Seguridad, Auditoría y Riesgos de TI
- Docente de Certificaciones CISA y CRISC en capítulos de ISACA.
- Docente de Maestrías en Auditorías y Seguridad de TI.
- Expositor y capacitador en Auditoría, Riesgos y Seguridad de TI.

Inversión y formas de pago

Día: 24, 25, 26 y 27 de marzo del 2026

Horario:

Zona Pacífico EEUU - **13:00**
Zona Montaña EEUU - **14:00**
Centroamérica, México y Zona Central EEUU - **15:00**
Perú, Panamá, Colombia, Ecuador y Zona Oriental EEUU - **16:00**
Rep. Dominicana, Bolivia y Venezuela - **17:00**
Brasil, Chile , Paraguay, Uruguay y Argentina - **18:00**
Guinea Ecuatorial - **22:00**

Costo:

Socios: USD 195,00 + IMP
No socios: USD 245,00 + IMP

Incluye:

- Asistencia al curso
- Material de apoyo
- Certificado de Participación
- Acceso al aula virtual

Pago del Curso:

Transferencias Bancarias
Banco intermediario Swift: CITIUS33. ABA: 021000089
Nombre: CITIBANK N.A.
Dirección: 111 Wall Street, New York, New York 10043
Transferir a Cuenta: 36026966. Swift: BSNJCRSJ.
Nombre: BAC San José (formerly Banco San José, S.A.)
Dirección: Calle 0 Avenidas 3 y 5, San José Costa Rica
Beneficiario Capacita Int S.A.
Cuenta Cliente: 10200009301147801
Cuenta IBAN: CR47010200009301147801
Cedula jurídica: 3-101-663566
IMPORTANTE: LA TRANSFERENCIA DEBE SER ENVIADA EN FORMATO MT103.
Favor remitir comprobante del deposito bancario escaneado al e-mail: info@capacita.co

Contáctenos

+506 4404 4859 / +506 6292 7902 / info@capacita.co / **www.capacita.co**