Capacita
e-Learning

Executive Internal Audit
Program

# Gestión de riesgos de TI con COSO, Cobit y la ISO 27005. Desde las 3 líneas de la organización

**6, 8, 13 y 14 de setiembre, 2022**
Programa online en vivo

**Wilson Andia Cuiza**

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

# Wilson Andia Cuiza

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

Tiene en su “ADN” Tecnología y Auditoría, con más de 20 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.
- 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.

# Descripción del Curso

## Introducción

La Tecnologías de la Información (TI) es un factor crítico de éxito para asegurar el logro de los objetivos institucionales y cada día más se depende de ella. Hemos depositando mucha confianza en la TI y nos encontramos en la era de la transformación digital por lo que la gran mayoría de los procesos están automatizados y la información procesada, almacenada y transportada por los sistemas interconectados, se ha convertido en el activo más valioso de las Instituciones.

Las organizaciones exitosas comprenden y gestionan los riesgos asociados con la implementación de nuevas tecnologías por lo que la identificación, evaluación, análisis y tratamiento de los Riesgos de TI e informar a la Alta Gerencia basados en marcos de control interno, metodologías y estándares alineados que incluyan a las Área de Tecnología y de Seguridad de la Información, es totalmente imprescindible para lograr los objetivos institucionales, como ser:

- Incrementar beneficios – ROI
- Mantener un riesgo aceptable
- Optimizar Costos
- Cumplir regulaciones
- Mantener Información de calidad
- Exigir confiabilidad y oportunidad de la información.
- Garantizar eficiencia y eficacia de las operaciones
- Disuadir, prevenir, detectar operaciones/transacciones inusuales que deriven en fraude informático.

## Objetivos

El objetivo del presente curso es describir los conceptos claves y el proceso de la Gestión de Riesgos de TI y su aplicación práctica desde la perspectiva de las 3 líneas de la organización, basado en marcos de control interno, metodologías y estándares internacionales alineados y que son de aceptación internacional considerados como mejores prácticas que permita coadyuvar al logro de los objetivos institucionales.

## Dirigido a

- Tecnologías de la información
- Seguridad de la información
- Riesgo Operativo (Riesgo Tecnológico)
- Finanzas
- Operaciones del Negocio
- Cumplimiento
- Continuidad
- Auditoría interna y externa

# Descripción del Curso

## Contenido

### Sesión 1

**Riesgos Tecnológicos y su Impacto en las Organizaciones**

- Peligros y riesgos informáticos que amenazan los sistemas y TI
- Amenazas, Fraudes y sabotajes informáticos (Tipos y formas)
- Tipos de ataques más comunes a TI
- Vulnerabilidades más comunes de TI en las organizaciones
- Efectos potenciales que pueden ocasionar los Riesgos de TI en las Organizaciones
- Técnicas de los atacantes
- Debilidades en las 3 líneas en las Organizaciones (nuevas 3 líneas del IAI).

### Sesión 2

**Marcos COSO, Gobierno y Gestión de TI COBIT 2019 y Estándar ISO 27005 para la Gestión de Riesgos de TI**

- Importancia del Gobierno de Riesgos Empresarial
- Importancia de la Gestión de Riesgos de TI
- Seguridad de la Información y Ciberseguridad
- Visión general de COSO
- Descripción general de COBIT 2019
- Entendiendo la ISO 27005
- Mapeo entre COSO, COBIT e ISO 27005 para la Gestión de Riesgos de TI

### Sesión 3

**Proceso de Gestión de Riesgos de TI con COSO, COBIT e ISO 27002**

- Identificando Riesgos de TI
- Evaluando Riesgos de TI
- Analizando Riesgos de TI
- Evaluando el Impacto de los Riesgos de TI
- Obteniendo matrices de Riesgos de TI
- Respondiendo a los Riesgos de TI (Tratamiento de Riesgos: Mitigar, Transferir, Aceptar, Evitar).
- Informe de Riesgos de TI a las partes interesadas (stakeholders).

### Sesión 4

**Aplicación práctica en las 3 líneas de defensa referente a Riesgos de TI**

- Aplicación del mapeo (COBIT, COSO e ISO 27005) en las nuevas 3 líneas
- Aplicación práctica en Tecnología de la Información
- Aplicación práctica en Seguridad, Riesgo, Cumplimiento y Continuidad
- Aplicación práctica en Auditoría de TI

# Inversión y Formas de Pago

**Día: 6, 8, 13 y 14 setiembre , 2022**

**Horario:**

**15:00 a 17:00 Centroamérica**

**Costo:**

**Socios:** USD 195,00 + IMP
**No socios:** USD 225,00 + 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

**Tel: (506) 2253-7631 / (506) 2234-0068 / info2@capacita.co / www.capacita.co**