Capacita
e-Learning

Executive Internal Audit Program

Auditoria forense informática en base a ISO 27037, aplicando software forense de investigación

12, 17, 19 y 24 de noviembre, 2020
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 19 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 señor 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

Las Entidades Privadas/Gubernamentales, reconocen la importancia de las Tecnologías de la Información (TI) y la consideran como 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.

Sin embargo, también existen diferentes riesgos tecnológicos a los que se afrontan las organizaciones ya sea externos e internos que deben ser mitigados metodológicamente y en algunas ocasiones los diferentes controles implementados o los esfuerzos realizados por las 3 líneas de defensa podrían no resultar exitosos o existir la complicidad o colusión entre algunos Empleados deshonestos que pueden originar y materializar el FRAUDE haciendo uso de medios tecnológicos, inclusive realizar el Fraude Informático en los Sistemas de Información.

En ese sentido, hace imperiosa la necesidad de contar con expertos en Auditoría Forense Informática o Peritos Forenses Informáticos que apoyen en la disciplina de la Auditoría Forense apegados a metodologías o estándares internacionales y sigan un proceso para que juntos en equipo puedan presentar a los Ejecutivos u órganos de control y judiciales la evidencia digital de quién, cuándo, cómo, dónde y que controles tecnológicos se vulneraron para cometer el ilícito y determinar la afectación reputacional o económica a la Organización.

En el presente curso son abordados aspectos o riesgos tecnológicos y las debilidades en las 3 líneas de defensa de la organización que podrían permitir los diferentes tipos de Fraudes. Así como las metodologías, estándares para la prevención, Auditoría Forense Informática y la investigación o detección del Fraude y el uso de herramientas/software forense. Estos aspectos podrían potenciar a los participantes dotándoles de las habilidades necesarias para colaborar en la lucha contra la corrupción, delitos y fraudes en sus organizaciones.

Objetivo

Empoderar y dotar de las capacidades técnicas a los participantes en metodologías, estándares y el uso de herramientas/software para la Auditoría Forense Informática y la Investigación del Fraude, así como metodologías y estándares para la prevención del Fraude en las 3 líneas de defensa de las organizaciones, generando de esta forma “valor agregado” para su Institución.

Descripción del Curso

Contenido

Primera Sesión:

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 de defensa

Segunda sesión

El Fraude y la Auditoría Forense Informática

- Tipos de Fraude
- El árbol del Fraude (clasificación)
- Tipificación de acciones que involucran alto riesgo de fraude y corrupción
- Prevención, detección e investigación de fraudes
- La Auditoría Forense Informática
- ¿Quiénes demandan este servicio?
- Objetivos de la auditoría forense
- Metodologías para la Auditoría Forense Informática
- Estándares para la Auditoría Forense Informática
- Una mirada a la ISO 27037
- El auditor forense informático características y requisitos
- Competencias que debe desarrollar el auditor forense

Tercera sesión

Herramientas/Software para la Auditoría Forense Informática

- La importancia de las evidencias digitales
- Recolección y Preservación de la Evidencia Digital
- Herramientas/Software para la obtención de Imágenes de Dispositivos de almacenamiento (Discos Duros, dispositivos USB, DVD)
- El procedimiento de copiado de discos
- La cadena de custodia
- Las buenas prácticas en el análisis
- Artefactos forenses, Data Carving y Metadatos
- Herramientas/Software para la Auditoría Forense Informática
- Herramientas/Software para el Análisis de Datos

Cuarta sesión

Claves para el Informe Pericial y presentación en Juicio y Caso Práctico

- El informe pericial
- Prueba anticipada en un proceso Civil
- Un Juicio Civil
- Claves de un forense en Juicio
- Caso práctico demostrativo usando Herramienta/software Forense
- Caso práctico demostrativo usando Herramienta/software para Análisis de Datos o CAATs

Inversión y Formas de Pago

- **Día: 12, 17, 19 y 24 de noviembre, 2020**
- **Costo: 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 / info@capacita.co / www.capacita.co