Capacita
e-Learning

Executive Internal Audit
Program

Auditoría del programa de ciberseguridad: NOGAI, NIST y la ISO 27032

2, 4, 9 y 11 de septiembre, 2025
15:00 Centroamérica
Programa online en vivo

Wilson Andia Cuiza

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

Descripción del Curso

Introducción

La ciberseguridad se ha convertido en un factor crítico de la gestión empresarial en la era digital para salvaguardar los activos de información, mantener la confianza de las partes interesadas, cumplir con regulaciones y minimizar riesgos cibernéticos y financieros. Además, es un componente esencial para la estrategia de crecimiento y sostenibilidad.

Las auditorías de ciberseguridad son procesos fundamentales para evaluar, fortalecer y mantener la seguridad de la información y los activos digitales en una organización, para garantizar:

- Protección contra amenazas en evolución.
- Cumplimiento normativo
- Protección de la reputación
- Reducción de riesgos financieros
- Optimización de recursos
- Resiliencia empresarial y continuidad de operaciones
- Protección de la propiedad intelectual
- Gestión proactiva de riesgos
- Sostenibilidad a largo plazo

Por lo mencionado, las auditorías de ciberseguridad son una inversión estratégica que protege los activos digitales de una empresa, garantiza el cumplimiento de normativas, reduce riesgos financieros y contribuye a la reputación y resiliencia empresarial

Objetivo

Fortalecer las competencias gerenciales, técnicas y mejores prácticas necesarias para verificar, revisar, evaluar, analizar y garantizar la seguridad de los sistemas, aplicativos, infraestructuras, redes y datos de una organización. Este curso está diseñado para proporcionar a los auditores y profesionales de seguridad de la información las habilidades y conocimientos necesarios para llevar a cabo auditorías de ciberseguridad efectivas basados en marcos y estándares actuales de Auditoría y Ciberseguridad y ayudar a las organizaciones a protegerse contra las amenazas cibernéticas.

Objetivo específico

- Identificar y analizar las principales ciberamenazas y actores maliciosos que afectan a las organizaciones, evaluando su impacto sobre los activos críticos de información.
- Comprender los aspectos claves de las Normas Globales de Auditoría Interna (NOGAI 2025) y el marco NIST 2.0 y la ISO/IEC 27032.
- Evaluar la alineación del programa de ciberseguridad con los objetivos estratégicos de la organización, verificando la existencia de una estructura de gobernanza y mecanismos de supervisión efectivos.
- Diseñar, planificar y ejecutar auditorías de ciberseguridad utilizando enfoques basados en riesgo, priorizando los controles críticos y la evidencia operativa.
- Aplicar metodologías de evaluación de madurez para diagnosticar el estado del programa y formular recomendaciones de mejora continua.
- Auditar procesos clave de ciberseguridad alineados con NIST 2.0 e ISO/IEC 27032.
- Verificar la capacidad operativa del programa para detectar, contener y recuperarse ante incidentes cibernéticos.

¿Porque Asistir?

- Aprenderás a auditar ciberseguridad con estándares internacionales de clase mundial
- Dominarás los marcos más relevantes y actuales como el NIST Cybersecurity Framework 2.0, la ISO/IEC 27032 y las NOGAI, aplicando prácticas que son reconocidas globalmente en auditorías y consultorías.
- Fortalecerás tu perfil profesional en un área de alta demanda y crecimiento
- La auditoría de ciberseguridad es hoy una competencia crítica. Este curso te posiciona como un profesional preparado para asumir roles clave en seguridad, auditoría interna, riesgos tecnológicos y cumplimiento.
- Adquirirás prácticas claves que un Auditor realiza para evaluar y mejorar programas de ciberseguridad
- Aprenderás cómo auditar procesos reales, identificar brechas, evaluar niveles de madurez y emitir recomendaciones concretas que aporten valor a la organización.
- Accederás a una formación impartida por un experto con más de 22 años de experiencia
- La experiencia del instructor en auditoría de TI, ciberseguridad y estándares internacionales garantiza una formación actualizada, aplicable y con casos prácticos del mundo real.

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 por las Normas Globales de Auditoría Interna (NOGAI 2025) y el NIST Cybersecurity Framework 2.0 así como la ISO/IEC 27032.

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 redacción de hallazgos y recomendaciones, orientados a mejorar la claridad, precisión y tono de los informes de auditoría de Ciberseguridad.
- Análisis de ejemplos reales y simulaciones, que permitirán aplicar técnicas efectivas para identificar hallazgos de Auditoría de Ciberseguridad adaptadas a distintos niveles organizacionales.

Descripción del Curso

- 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 estadísticas de ciberseguridad, Normas Globales de Auditoría Interna (NOGAI 2025) y el NIST Cybersecurity Framework 2.0 así como un preview de la ISO/IEC 27032.

Dirigido a:

- Auditores Internos
- Auditores Externos
- Miembros de Comités de Auditoría
- Tecnologías de la información
- Seguridad Cibernética y de la información
- Riesgo Operativo (Riesgo Tecnológico)
- Cumplimiento
- Continuidad

Contenido

Las Ciberamenazas y los actores maliciosos

- ¿Qué es la Ciberseguridad y en qué se diferencia a la Seguridad de la Información?
- Estadísticas de Ciberseguridad, Ciberamenazas y los actores maliciosos más importantes.
- Tipos de Ciberamenazas y actores maliciosos más comunes.
- Vulnerabilidades de Ciberseguridad más comunes en las organizaciones.
- Casos relevantes de ataques Cibernéticos.
- Roles y responsabilidades en las 3 líneas de la organización referente a Ciberseguridad.

Conociendo, comprendiendo las NOGAI y los Marcos de Ciberseguridad NIST y la ISO 27032 y utilizando un modelo de nivel de madurez

- Aspectos claves de las NOGAI
- Comprendiendo el Marco de Ciberseguridad NIST
- Entendiendo la ISO 27032 de Ciberseguridad
- Mapeo entre NIST y la ISO 27032
- Aplicando el Modelo de Madurez de NIST y la ISO 27032
- Gobierno y Gestión del Programa de Ciberseguridad

El Proceso y la documentación de la Auditoría de Ciberseguridad

- Iniciando una Auditoría de Ciberseguridad
- Fase de relevamiento de información
- Fase de realización de análisis de riesgos cibernético
- Fase de Planificación de la Auditoría de Ciberseguridad
  - Elaboración del Programa de Auditoría de Ciberseguridad
  - Elaboración de los Procedimientos de Auditoría, ChekList, Cuestionarios a utilizar en la Auditoría de Ciberseguridad
- Fase de Ejecución de la Auditoría (trabajo de campo)
  - Atributos de la evidencia de Auditoría de Ciberseguridad
  - Aspectos claves a considerar para obtener la evidencia
- Fase de elaboración del Informe borrador de Auditoría de Ciberseguridad
- Fase de Seguimiento de la Auditoría de Ciberseguridad (Auditoría posterior)
- Ejemplos de redacción de hallazgos y recomendaciones, orientados a mejorar la claridad, precisión y tono de los informes de auditoría de Ciberseguridad

Auditando procesos claves de la Ciberseguridad basado en NIST y la ISO 27032

- Auditando los Procesos Auditando las prácticas de gestión de activos, vulnerabilidades, cambios, configuración, parches.
- Auditando los controles de Ciberseguridad en las plataformas.
- Auditando las prácticas de gestión de seguridad de redes e infraestructura de comunicaciones.
- Auditando los controles de ciberseguridad de aplicaciones y bases de datos.
- Auditando la ciberseguridad de servicios en la nube.
- Auditando procesos claves como:
  - Identificación (NIST CSF Function - Identify)
  - Protección (NIST CSF Function - Protect)
  - Detección (NIST CSF Function - Detect)
  - Respuesta (NIST CSF Function - Respond)
  - Recuperación (NIST CSF Function - Recover)
  - Gestión de Riesgos (NIST Core - Risk Management)
  - Gestión de la Autenticación y la Identidad (NIST Core - Identity and Access Management)
  - Seguridad de Red (NIST Core - Network Security)
  - Gestión de Activos (NIST Core - Asset Management)
  - Gestión de Vulnerabilidades (NIST Core - Vulnerability Management)
  - Seguridad de la Información y Documentación (NIST Core - Information and Documentation)
  - Seguridad de Aplicaciones/Sistemas (NIST Core - System Security)
  - Educación y Concienciación (NIST Core - Awareness and Training)
  - Evaluación y Medición (NIST Core - Assessment and Measurement)
  - Gestión de Proveedores (NIST Core - Supply Chain Risk Management)
  - Desarrollo Seguro (NIST Core - Secure Development)

Wilson Andia Cuiza

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

Tiene en su "ADN" Tecnología y Auditoría, con más de 22 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: 2, 4, 9 y 11 de septiembre, 2025

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, Chile, Bolivia y Venezuela - 17:00
Brasil, 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

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