ISACA Costa Rica Chapter

CYBERSECURITY FUNDAMENTALS An ISACA Certificate

CURSO OFICIAL PARA LA CERTIFICACIÓN EN FUNDAMENTOS DE CIBERSEGURIDAD DE ISACA

Objetivo:

Promover en los participantes el desarrollo de conocimientos teóricos y habilidades prácticas relacionadas y utilizadas para el gobierno y gestión de la Ciberseguridad, preparándolos para optar por la certificación en Fundamentos de Ciber Seguridad de ISACA® (CSXF), la cual forma parte del programa Information Technology Certified Associate (ITCA).

Público Meta:

- Estudiantes o graduados de carreras relacionadas con las tecnologías de información
- Profesionales que desean desarrollar experiencia y capacidades en ciberseguridad.
- Profesionales de especialidades no tecnológicas que desean hacer carrera en ciberseguridad

Modalidad: Virtual (ZOOM)

Fecha: del 23 al 27 de mayo del 2022

Sesiones: 5 Sesiones

Hora: 6:00 pm a 9:30 pm.

Horas CPE´s: 16 horas.

Qué incluye este curso:

- Presentación utilizada durante el curso en PDF
- Enlaces a información de Internet
- Guías para el taller práctico
- Certificado de participación

Contenido:

Fundamentos de seguridad

1.1 Objetivos de aprendizaje
1.2 Descripción general
1.3 ¿Qué es la seguridad?
1.4 Tipos de seguridad
1.5 Sistemas especializados
1.6 Roles y responsabilidades
1.7 Gobierno, gestión de riesgos y cumplimiento
1.8 Gobernanza de la ciberseguridad
1.9 Resiliencia
1.10 Continuidad del negocio y recuperación ante desastres
1.11 Análisis de impacto en el negocio
1.12 Conceptos de recuperación
1.13 Objetivos de seguridad de la información
1.14 Privacidad
1.15 Privacidad vs seguridad

Comprendiendo el panorama de amenazas

2.1 Objetivos de aprendizaje
2.2 Riesgo de ciberseguridad
2.3 Amenazas
2.4 Vulnerabilidades
2.5 Ciberataques
2.6 Atributos de ataque
2.7 Proceso de ataque
2.8 Códigos maliciosos y ataques
2.9 Evaluación de riesgos
2.10 Consideraciones sobre la cadena de suministro
2.11 Ciclo de Vida de la Gestión de Riesgos
2.12 Gestión del riesgo
2.13 Uso de los resultados de las evaluaciones de riesgos

Asegurando activos

3.1 Objetivos de aprendizaje
3.2 Identificación de riesgos, estándares, marcos y orientación de la industria
3.3 Arquitectura, modelos y marcos
3.4 Controles de seguridad
- 3.4.1 Tipos de controles
- 3.4.2 Documentos de cumplimiento y marcos de políticas
- 3.4.3 Funciones de control
- 3.4.4 Recursos de control
- 3.4.5 Evaluación de los controles de seguridad
- 3.4.6 Gestión de acceso e identidad
- 3.4.7 Seguridad de la red
- 3.4.8 Seguridad de punto final
- 3.4.9 Configuración segura del sistema
- 3.4.10 Registro, Monitoreo y Detección
- 3.4.11 Seguridad de la aplicación
- 3.4.12 Seguridad en la nube
- 3.4.13 Seguridad de los datos
- 3.4.14 Gestión de la configuración
- 3.4.15 Gestión de cambios
- 3.4.16 Gestión de parches
- 3.4.17 Fundamentos, técnicas y aplicaciones de cifrado

Operación y respuesta de ciberseguridad

4.1 Objetivos de aprendizaje
4.2 Operación de ciberseguridad
- 4.2.1 Centros de Operaciones de Seguridad (SOC)
- 4.2.2 Principales áreas de ciberseguridad
- 4.2.3 Gestión de vulnerabilidades
- 4.2.4 Prueba de intrusión
- 4.2.5 Pruebas de intrusión vs análisis de vulnerabilidades
- 4.2.6 DevOps y DevSecOps

4.3 Herramientas y tecnologías (monitoreo, detección, correlación)
4.4 Manejo de incidentes
4.5 Análisis forense digital

Instructor:

Raúl Rivera Méndez

CISA, CGEIT, CRISC, CSIM, CSXF, CDPSE, CSXF, CSXA, COBIT5F, ITILF, ISO27001 AL, DFIR, CSFPC, KIKF, RWPC, SFPC

Profesional con más de 27 años de carrera profesional y experiencia en el sector financiero, servicios y de las tecnologías de la información y comunicación, el cual ha laborado para importantes empresas transnacionales como Acer, Unisys, PwC, BAC Credomatic y Mastercard. Ha sido miembro de la Junta Directiva de ISACA Costa Rica y actualmente es asesor y vocero en ciberseguridad para la Asociación Bancaria Costarricense. Lidera para Costa Rica el programa de Cybersecurity Nexus de ISACA y el Centro de Ciberseguridad Industrial de España. Ha colaborado para la Organización de Estados Americanos capacitando en Ciberseguridad a personal de gobiernos latinoamericanos, así como en el desarrollo de propuestas de políticas públicas para parlamentos latinoamericanos. Cuenta con más de 18 años de experiencia como conferencista internacional en Seguridad de la Información y Ciberseguridad, además de ser instructor acreditado por AMPG Internacional para cursos oficiales de ISACA Global.

Inversión:

- Asociados $ 185.00
- Colegiado CPIC $ 285.00
- Público General $ 325.00

***Precios Incluyen IVA.**

Formas de pago:

- ✓ Transferencia
- ✓ Depósito a la cuenta de Asociación Costarricense de Auditores en Informática

- **A Nombre de la Asociación Costarricense de Auditores en Informática.**
- **Cédula Jurídica:** 3-002-045936

Cta. IBAN Colones -BCR CR69015201001013860853
Cta. IBAN Dólares - BCR CR96015201001022338943

Nota:

Enviar copia del depósito / comprobante de transferencia a la cuenta electrónica capacitacion@isacacr.org

Información adicional:

ISACA ofrece también su paquete de laboratorio de fundamentos de ciberseguridad.

Descripción del Laboratorio:

"Cybersecurity Fundamentals Practice Labs" ofrece a los estudiantes la oportunidad de ampliar y demostrar su comprensión y capacidad para desempeñarse en los entornos empresariales y de TI amenazados por la ciberseguridad de hoy. Demuestre competencia práctica de herramientas de seguridad, amenazas y vulnerabilidades, describa procesos y prácticas de gestión de riesgos y más a su ritmo, en cualquier momento y en cualquier lugar.
El paquete de laboratorio interactivo y autoguiado se centra en la formación basada en el rendimiento. Esta aplicación práctica brinda una experiencia de aprendizaje única y dinámica que desarrolla y refuerza las habilidades críticas necesarias para realizar muchas de las tareas técnicas vitales para su éxito en el campo de TI.

Laboratorios incluidos en este paquete:

- Cortafuegos para sistemas operativos Windows y Linux
- Escaneo de puertos y uso de SSH
- Línea base con Lynis
- Análisis forense: recuperación de archivos
- Permisos de archivo en Windows y Linux
- Detección de amenazas
- Eliminación de amenazas
- Supervisión y defensor de eventos de Windows
- Inyección SQL

Los alumnos tendrán acceso al curso durante un año a partir de la fecha de compra y obtendrán 9,5 CPE al finalizar. Este laboratorio tiene un tiempo de aplicación de aproximadamente 8 horas.

Costos de los laboratorios:

- $ 136 dólares para miembros
- $200 dólares para NO miembros

En el siguiente enlace pueden ver más información:

https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Koh7EAC

Información sobre el examen de certificación:

No hay requisitos previos. Puede registrarse para el examen en cualquier momento. El examen en línea de 2 horas supervisado de forma remota **combina conocimientos (opción múltiple) y preguntas basadas en el desempeño** establecidas en un entorno de laboratorio virtual.

Para aprobar el examen, debe obtener un puntaje de 65% o más

Costos del examen

- $ 120 dólares para miembros
- $150 dólares para NO miembros

Idioma del examen:

- Inglés