Taller práctico para la Gestión y Gobierno de Riesgos de Seguridad de la Información y Ciberseguridad.

Taller Práctico para la Gestión y Gobierno de Riesgos de Seguridad de la Información y Ciberseguridad.

Modalidad: Virtual (ZOOM)

Fecha: lunes 19, miércoles 21, viernes 23, lunes 26, miércoles 28 ,Viernes 30 de mayo y lunes 02 de Junio.

Sesiones: 7 Sesiones

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

Horas CPE´s: 21 horas.

Objetivo:

Este es un taller teórico práctico, de nivel cero a experto.

Le brindará al participante la oportunidad de complementar los conocimientos teóricos técnicos de la administración del riesgo de seguridad de la información, con una serie de plantillas y ejercicios prácticos que le permitan no sólo comprender los temas más relevantes dentro de un proceso de gobierno y gestión del riesgo de seguridad de la información, sino que sobre cómo abordar una posible estrategia de implementación paso a paso.

Curso Incluye:

- Material de Referencia
- Certificado de participación

Contenido:

1. Introducción a la seguridad de la información

- La información y su importancia
- Riesgos de seguridad de la información
- Relación entre los riesgos de SI, con otros tipos de riesgos
- Impactos o consecuencias de la materialización de riesgos de SI
- Evolución del panorama de riesgos de SI
- El verdadero valor de nuestra información
- Explorando el estado de la situación actual

2. Proceso de gestión de riesgos

- El proceso de gestión de riesgos
- Objetivos de la gestión de riesgos
- Integralidad de la gestión de riesgos
- Roles y responsabilidades en la gestión de riesgos
- Identificación y redacción de riesgos
- Cuantificación de los riesgos
- Apetito y tolerancia a los riesgos
- Diseñando indicadores de monitoreo de riesgos
- Definiendo planes de tratamiento de riesgos
- Diseño e implementación de controles
  - Protegiendo la Confidencialidad
  - Protegiendo la Integridad
  - Protegiendo la Disponibilidad

3. Gestión de eventos e incidentes de SI

- Diferencias entre un evento y un incidente de SI
- Reportando eventos e incidentes de SI
- Diferencias entre incidentes e incidencias
- Lecciones aprendidas de los eventos e incidentes de SI
- Activos de información y su importancia
- Formatos de activos de información
- La información y su ciclo de vida
- Activos de soporte a la información
- Clasificando y valorando la información
- Gestionando los activos de información

5. Gobierno y gestión de la seguridad de la información

- Diferencias entre el gobierno y la gestión de la SI
- Implementando un proceso de gobierno y gestión de SI
- La importancia de las líneas de defensa
- Amenazas de SI
- Vulnerabilidades de SI
- Afectación a la CID de los activos de información
- Identificando los riesgos de SI

6. Pruebas de autoevaluación de controles (CSA)

- Proceso de autoevaluación de controles
- Diseñando una prueba de autoevaluación de controles
- Documentando los resultados

7. Conclusiones

- El CISO y su importancia
- Principales capacidades que debe tener un CISO
- Conclusiones Finales.

Instructor:

Raúl Rivera Méndez
CISA – CISM – CRISC – CGEIT – CDPSE – CSXF – CSXA – COBIT 5F – ITILF – AL ISO27001 – CCISO – DFIR

El instructor es Bachiller en Ingeniería Informática, Máster en Telemática, Máster en Administración de Empresas con énfasis en Finanzas y Máster Profesional en Ciberseguridad Industrial.
A lo largo de sus 30 años de carrera profesional, se ha especializado en la gestión de riesgos operativos, seguridad de la información, riesgos tecnológicos, continuidad de negocios y ciberseguridad. Ha acumulado experiencia en diversos sectores como el financiero, servicios y de tecnologías de la información, trabajando para destacadas compañías transnacionales como Acer, Unisys, PwC, BAC y Mastercard. Actualmente, es CEO y fundador de Cyber-C, una empresa dedicada a la asesoría y consultoría en gestión de riesgos y ciberseguridad.
Lidera en Costa Rica los programas Cybersecurity Nexus de ISACA y el Centro de Ciberseguridad Industrial de España. Ha colaborado con la OEA, capacitando a gobiernos latinoamericanos y desarrollando políticas públicas de ciberseguridad para parlamentos latinoamericanos, así como con el Ministerio de Ciencia, Tecnologías y Telecomunicaciones (MICITT) en la actualización de la Estrategia de Seguridad Nacional y las Normas Técnicas.
Cuenta con más de 20 años de experiencia como conferencista internacional. Es instructor certificado para impartir los cursos oficiales de certificación en Fundamentos de Ciberseguridad (CSXF) y Auditoría de Ciberseguridad (CSXA) de ISACA a nivel internacional.
Ha sido asesor en ciberseguridad y fraude para la Superintendencia General de Entidades Financieras (SUGEF), asesor y vocero en ciberseguridad para la Asociación Bancaria Costarricense (ABC), miembro de la Junta Directiva de la Oficina del Consumidor Financiero de Costa Rica (OCF), miembro de Junta Directiva de International Information System Security Certification Consortium (ISC2) capítulo Costa Rica. ex-miembro de Junta Directiva de Information Systems Audit and Control Association (ISACA) capítulo de Costa Rica

Inversión:

- Asociados ₡ 130 000 colones
- Colegiado ₡ 170 000 colones
- Público General ₡ 190 000 colones

***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 al correo capacitacion@isacacr.org