Universidad del Rosario | Educación Continua y Consultoría

CERTIFIED CHIEF INFORMATION SECURITY OFFICER (C |CISO)

CONTENIDO TEMÁTICO

Módulo 1 - GOBERNANZA Y GESTIÓN DE RIESGOS

1.Programa de gobernanza en seguridad de la información.
2.Objetivos de seguridad de la información.
3. Establecimiento de una estructura de gestión de seguridad de la información.
4.Leyes, regulaciones y estándares.
5.Políticas de seguridad.
6.Código de ética del EC-Council.
7.Gestión de riesgos de seguridad

Módulo 2 - CONTROLES DE SEGURIDAD, COMPLIANCE Y GESTIÓN DE AUDITORIA

1.Controles de seguridad de la información.
2.Madurez en los controles de seguridad.
3.Catálogo de servicios de seguridad de la información.
4.Gestión de compliance.
5.Regulaciones y estándares: GDPR, ISO27000, PCI DSS, NIST.
6.Guías y buenas prácticas: CIS, OWASP.
7.Gestión de auditoría.

Módulo 3 - GESTIÓN DE UN PROGRAMA DE SEGURIDAD

1. Gestión de un programa de seguridad.
2. Objetivos, requerimientos, stakeholders, y desarrollo de la estrategia de un programa de seguridad.
3. Recursos humanos en un programa de seguridad.
4. Gestión de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP).
5. Plan de respuesta a incidentes.
6. Gestión de operaciones.
7. SIEM (Security Information and Event Management).

Módulo 4 - CONCEPTOS PRINCIPALES DE SEGURIDAD DE LA INFORMACIÓN

1. Control de acceso y arquitectura AAA.
2. Riesgos de seguridad física.
3. Arquitectura de seguridad de redes.
4. Protección de endpoints: PC, smartphones y dispositivos IoT.
5. Seguridad en el Ciclo de desarrollo de Software: DevSecOps.
6. Tecnologías de cifrado: criptosistemas, algoritmos.
7. Seguridad de virtualización y modelos de referencia.
8. Seguridad en la nube.

Módulo 5 - GESTIÓN ESTRATÉGICA, FINANCIERA Y DE PROVEEDORES

Módulo 5 - Gestión estratégica, financiera y de proveedores

1. Planeación estratégica.
2. Diseño, desarrollo y mantenimiento de un programa de seguridad de la información.
3. Arquitectura Empresarial.
4. Gestión financiera.
5. Programa de adquisiciones.
6. Gestión de proveedores.
8. Threat Intelligence.
9. Gestión de vulnerabilidades.