

ELECTIVA: SEGURIDAD INFORMÁTICA	
Intención Curricular	La unidad curricular Seguridad Informática permitirá al estudiante adquirir conocimientos inherentes a la formulación y aplicación de políticas de seguridad informática organizacional basada en normas y legislaciones nacionales e internacionales.
Conocimientos previos	Haber aprobado el trayecto III y los dos primeros módulos de la Unidad Curricular Formación Sociopolítica IV.
Duración	Un Trimestre 12 semanas académicas, con 9 horas semanales a invertir, 3 horas de encuentro con el Profesor - Asesor y 6 horas de estudios independientes y consulta. Las horas de encuentro con el profesor asesor se consideran horas académicas de 45 minutos cada una.
Créditos Académicos	Tres (3) créditos académicos
Material Instruccional	Módulos instruccionales para cada trimestre en formato electrónico e impreso, direcciones electrónicas, videos, CD entre otros.
Estrategias Instruccionales	Encuentros Semanales, Trabajos individual o en Grupo, Estudio Independiente, Consultas.
Recursos Requeridos	Material Instruccional y Didáctico. Laboratorios de computación para actividades prácticas.
Contenido	<p>Módulo I: Introducción a la Seguridad Informática: Definición. Términos asociados. Retos de la seguridad Informática. Motivaciones para implementar mecanismos de seguridad. Sistemas de Seguridad, elegir un nivel de seguridad apropiado. Seguridad Física / Lógica: Amenazas potenciales. Tipos de desastres, Acciones hostiles, Disponibilidad, Integridad, Confidencialidad, Control de accesos. Denegación de servicio. Virus: Troyanos, Gusanos, Backdoors, Espías, entre otros. Intercepción de datos confidenciales. SPAM, SCAM. Sitios Web Ficticios. Legislación: Legislación Internacional, Amenazas humanas, Amenazas lógicas, Protección. Identificar las características y aplicación de las normas ISO 27001, ISO 17799, COBIT, NIST y Systrust y Webtrust de AICPA (The American Institute of Certified Public Accountants).</p> <p>Módulo II: Estrategias, metodologías y Procedimientos: Análisis de Riesgos. Revisión y Auditoría de la Infraestructura actual, Detectar Intrusiones. Plan de Recuperación de Incidentes. Implementar acciones correctoras. Métodos de Cifrado: Criptografía; Criptosistemas (de clave secreta, de Cifrado en flujo, de clave pública). Identificar los principios matemáticos para criptografía simétrica y asimétrica. Esteganografía: Técnicas según el medio (en texto, imágenes, audio y video). Funciones de autenticación, Describir el funcionamiento de los algoritmos DES, 3DES, AES, RSA utilizados en seguridad informática. Servicios AAA: Identificar las ventajas que ofrece el uso de servicio Radius,</p>

	<p>TACACS y Kerberos. Identificar las principales características de los algoritmos de Hash MD5 y SHA-Firma digitales y certificados digitales. Políticas de seguridad: Políticas de seguridad informática. Implementación de políticas de seguridad. Firewall y técnicas de implementación. Evaluación de riesgos. Estrategia de seguridad.</p>
<p>Referencias Bibliográfica</p>	<ol style="list-style-type: none">1. Royer, J. Seguridad en la Informática de Empresa. Riesgos, amenazas, prevención y soluciones. Eni Ediciones, Francia. 2004.2. Firtman, S. Seguridad Informática: Amenazas y Vulnerabilidades más Peligrosas, al Desnudo. MP Ediciones. Manuales Users. Sept. 1, 2005.3. Gómez, A. Enciclopedia de la Seguridad Informática. Alfaomega. RA-MA. México, 2008.4. Ley Especial Contra los Delitos Informáticos5. Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas6. Ley Sobre Derecho de Autor