

UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

SECRETARÍA GENERAL

FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

**DESCRIPCIÓN DE CURSO DE LA CARRERA DE
MAESTRÍA EN SEGURIDAD INFORMÁTICA**

2014

**APROBADO POR EL CONSEJO DE INVESTIGACIÓN, POSTGRADO Y EXTENSIÓN EN
REUNIÓN N° 03-2014, DEL 9 DE ABRIL DE 2014.**

**"Secretaría General dispone de un Sistema de Gestión de la Calidad certificado de acuerdo a la norma
ISO 9001:2008 por Applus+ Certification Technological Center".**

UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
SECRETARÍA GENERAL
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

DESCRIPCIÓN DE CURSO: MAESTRÍA EN SEGURIDAD INFORMÁTICA

Asignatura: SISTEMAS DE SEGURIDAD I

Código de asignatura: S001

Horas semanales de clases: 3

Total de créditos: 3

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Se tratarán los siguientes tópicos: objetivos de la seguridad de redes, principales formas de ataques, arquitectura de protocolos TCP/IP y sus principales problemas de seguridad. Este curso conlleva prácticas de laboratorio para el reforzamiento de conceptos, y para el desarrollo de habilidades y destrezas en el manejo de herramientas de seguridad.

Asignatura: CRIPTOGRÁFIA Y SUS APLICACIONES

Código de asignatura: S002

Horas semanales de clases: 3

Total de créditos: 3

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Este curso explora principios de cifrado, conceptos criptográficos, criptografía de clave simétrica y asimétrica, estándares de encriptación, DES, 3DES, AES, RSA, cipher block chaining; cipher feedback mode; funciones hash; firma digital. Así mismo, se tocarán temas relacionadas con las aplicaciones con el cifrado, tales como SSH, HTTPS--SSL/TLS, IPSEC, VPN, Correo Seguro--PGP, esteganografía y marcas de agua digitales, entre otros. Además de IPSEC, VPN, PKI, cifrado de datos en reposo y en tránsito, entre otros. Este curso conlleva prácticas de laboratorio para el reforzamiento de conceptos, y para el desarrollo de habilidades y destrezas en el manejo de herramientas de seguridad.

Asignatura: SISTEMAS DE SEGURIDAD II

Código de asignatura: S003

Horas semanales de clases: 3

Total de créditos: 3

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Se tratarán temas tales como: diseños básicos para redes seguras, (DMZ, Firewall, IDS/IPS, Honeypots, monitoreo de bitácoras, entre otros), defensa en profundidad, gestión de vulnerabilidades y manejo de parches. Este curso conlleva prácticas de laboratorio para el reforzamiento de conceptos, y para el desarrollo de habilidades y destrezas en el manejo de herramientas de seguridad.

Asignatura: SEGURIDAD EN SISTEMAS OPERATIVOS

Código de asignatura: S004

Horas semanales de clases: 3

Total de créditos: 3

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Se cubrirán los sistemas Microsoft Windows, *nix, servicios y procesos, aplicaciones de redes y números de puerto, Tcp-Wrappers, Host-IDS/IPS, firewalls personales, controles de accesos, políticas en directorios activos, configuración del registry, líneas base y plantillas de seguridad, bloqueo y monitoreo de puertos USB, almacenamiento y rompimientos de contraseñas en los sistemas operativos, rastreo de puertos y vulnerabilidades y aplicación de parches y medidas correctivas.

Este curso conlleva prácticas de laboratorio para el reforzamiento de conceptos, y para el desarrollo de habilidades y destrezas en el manejo de herramientas de seguridad.

Asignatura: **SEGURIDAD MÓVIL**

Código de asignatura: S005

Horas semanales de clases: 3

Total de créditos: 3

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Conocer las debilidades y amenazas de seguridad móvil. Describir cómo los atacantes pueden utilizar los dispositivos móviles para abusar y atacar una organización. Además, explicará la arquitectura de un sistema móvil, seguridad y ataques a GSM, UMTS y demás, vulnerabilidades en servicios móviles, ataques jamming a celulares y mitigación, seguridad en servicios de VoIP a celulares, seguridad en aplicaciones móviles, seguridad en IP móvil, seguridad en sistemas operativos móviles tales como Android, iOS (iPad, iPhone), Windows Phone, Blackberry, Symbian OS.

Este curso conlleva prácticas de laboratorio para el reforzamiento de conceptos, y para el desarrollo de habilidades y destrezas en el manejo de herramientas de seguridad.

Asignatura: **SEGURIDAD EN BASE DE DATOS**

Código de asignatura: S006

Horas semanales de clases: 3

Total de créditos: 3

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Se tratarán los conocimientos básicos de los principales motores de bases de datos relacionales--SQL Server, Oracle, MySQL, Sybases, IBM DB2, Postgress; instalación y formas de acceso a las bases de datos --- línea de comando, vía web, aplicación de consultas y configuración, creación de objetos, usuarios, tablas, campos; creación de consultas en SQL; asignación de roles y privilegios/permisos; copias de respaldo; procedimientos almacenados y triggers; herramientas de monitoreo continuo y firewalls para bases de datos; principales amenazas y vulnerabilidades en bases de datos y mejores prácticas de seguridad en BD.

Este curso conlleva prácticas de laboratorio para el reforzamiento de conceptos, y para el desarrollo de habilidades y destrezas en el manejo de herramientas de seguridad.

Asignatura: **APLICACIONES SEGURAS**

Código de asignatura: S007

Horas semanales de clases: 3

Total de créditos: 3

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Se tratarán temas tales como: uso de plantillas prácticas y métodos para administrar la seguridad, las formas para mantener la integridad en ambientes de sistemas en usos. Se incluirán técnicas para manejar seguridad a través de una variedad amplia de arquitecturas desarrolladas tales como: SAVIA, Peoplesoft, Oracle, y JD Edwards. También se tratarán sobre el porqué de las aplicaciones seguras, diseño seguro, manejo de soluciones para páginas Web: Protección de los sitios web, vulnerabilidades en página web, SSL.

Desarrollo y gestión de sitios Web: HTML, DHTML, JavaScript, CGI's, PHP, ASP, JSP, HTTPS, Autenticación, WebDAV, presentaciones en FLASH. XML, acceso a base de datos a través de Internet (JDBC, ODBC).

Este curso conlleva prácticas de laboratorio para el reforzamiento de conceptos, y para el desarrollo de habilidades y destrezas en el manejo de herramientas de seguridad.

Asignatura: **ÉTICA Y LEGISLACIÓN EN SEGURIDAD INFORMÁTICA**

Código de asignatura: S008

Total de créditos: 2

Horas semanales de clases: 2

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Se presenta los derechos penales nacionales e internacionales por delitos informáticos, mal uso de computador. Además, como los organismos internacionales buscan y señalan los casos cuando el problema se eleva a la escena internacional, cuáles son los inconvenientes que se enfrentan, la regulación de la problemática de la cibernética y su utilización tan generalizada en el mundo. Además, se presentan ejemplos de legislación en otros países.

Esto incluye influencia de la legislación en la estructura informática, LOPD, LSS, código penal en general, legislación frente a delitos informáticos, legislación internacional, leyes y regulaciones nacionales, paraísos legales e intrusos informáticos, delitos: Informáticos, No informáticos y Mixtos, tipos de atacante y motivaciones, CERT (centros de emergencia) y policía judicial, qué hacer frente a un incidente de seguridad.

Asignatura: **GESTIÓN DE INCIDENTES DE SEGURIDAD**

Código de asignatura: S009

Total de créditos: 2

Horas semanales de clases: 2

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Se cubrirán tópicos relacionados con clasificación de incidentes de seguridad, normas de seguridad para la gestión de incidentes, directrices y procedimientos, notificación y detección de incidentes de seguridad, manejo y respuesta ante los incidentes, recolección y conservación de las pruebas, sucesos relacionados con información de identidad confidencial, reportes y seguimiento de incidentes.

Este curso conlleva prácticas de laboratorio para el reforzamiento de conceptos, así mismo en el desarrollo de habilidades y destrezas en el estudiante en herramientas de seguridad.

Asignatura: INFORMÁTICA FORENSE

Código de asignatura: S010

Horas semanales de clases: 3

Total de créditos: 3

Horas semanales de laboratorio: 0

DESCRIPCIÓN: En este curso se describe la forma de detectar el crimen por computadora, seguir a un criminal, forma de detectarlos, tácticas de investigación, responsables del análisis forense y montaje de la evidencia del delito informático. Cibercrimen y leyes relacionadas a delitos informáticos y a la recolección de pruebas; Evidencia digital, cadena de custodia, informática forense en computadoras (discos duros, memoria ram), teléfonos móviles, otros equipos de comunicación (switches, routers), análisis de memoria y detección de malware), uso de herramientas para rompimiento de contraseñas, detección de archivos con esteganografía); efectos y resultados de incidentes causados por cibercrimen.

Este curso conlleva prácticas de laboratorio para el reforzamiento de conceptos, y para el desarrollo de habilidades y destrezas en el manejo de herramientas de seguridad.

Asignatura: TÓPICOS ESPECIALES

Código de asignatura: S011

Horas semanales de clases: 2

Total de créditos: 2

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Formulación y Dirección de Proyectos de Seguridad. Seguridad en Sistemas Distribuidos. Seguridad en Data Center. Seguridad en Cloud Computing. Seguridad en Telefonía IP. Técnicas Hacking. Técnicas Biométricas.

Asignatura: ADMINISTRACIÓN DE LA SEGURIDAD INFORMÁTICA

Código de asignatura: S012

Horas semanales de clases: 3

Total de créditos: 3

Horas semanales de laboratorio: 0

DESCRIPCIÓN: Se tratará sobre el conocimiento de la infraestructura de la red, Mejores prácticas en el establecimiento de una oficina de seguridad informática y sus operaciones (defensivas y ofensivas), Análisis y Evaluación de Riesgos y metodologías OCTAVE-MEHARI-MAGERIT-NIST-Microsoft; Concienciación y Educación en Seguridad de la información; Políticas de seguridad, gestión de los controles de acceso y contraseñas, gestión de la propiedad intelectual, responsabilidad legal, contratación de personal de seguridad y certificaciones, Preparación de un programa/estrategia de seguridad, convergencia entre seguridad lógica y física.

Este curso conlleva prácticas de laboratorio para el reforzamiento de conceptos, y para el desarrollo de habilidades y destrezas en el manejo de herramientas de gestión de seguridad.

Asignatura: TESIS

Código de asignatura: S013

Horas semanales de clases: 6

Total de créditos: 6

Horas semanales de laboratorio: 0