.UBAeconómicas posgrado

ENAP Escuela de Negocios y Administración Pública

EXACTAS UBA FACULTAD DE INGENIERIA Universidad de Buenos Aires

MAESTRÍA Y ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA

CONTENIDOS MÍNIMOS:

1. Ejes temáticos de la seguridad

Hoja de ruta de la maestría. Concepto de seguridad. Servicios básicos de seguridad. Elementos a proteger. Amenazas, riesgos, vulnerabilidades. El factor humano. Revisión de los conocimientos necesarios de matemática discreta sobre los cuales se desarrolla la criptografía contemporánea. Revisión y actualización de los conocimientos necesarios de tecnología de la información: bases de datos; sistemas operativos, redes. Revisión y actualización de los conocimientos necesarios de gestión de las organizaciones: conceptos, técnicas y herramientas. Aspectos éticos y legales. Auditoría y análisis forense.

2. Criptografía I

Fundamentos de criptología. Introducción a los criptosistemas. Criptología clásica: cifrados y ataques. Secreto perfecto y One-Time Pad. Criptosistemas simétricos: históricos y actuales; modos operativos. Criptosistemas asimétricos; comparaciones de seguridad entre cifradores simétricos y de clave pública. Gestión de claves simétricas y asimétricas. Intercambio seguro de claves. Funciones Hash/ MAC/HMAC. Generación de números aleatorios. Ataques. Protocolos especiales.

3. Gestión estratégica de la seguridad I

Organización y estructura del área de seguridad: áreas, funciones y responsabilidades, perfiles, criterios de organización. Técnicas de gestión (estrategia, finanzas, marketing y recursos humanos). Ciclo de vida de los sistemas de seguridad. Gestión de proyectos de seguridad. Tercerización de servicios y gestión de proveedores. Evaluación económica de la seguridad. Métricas y performance. Estrategias, políticas, programas y normas de seguridad. Introducción al análisis y gestión del riesgo.

4. Seguridad en redes I

Esquemas de Seguridad: distribución de claves simétricas. Administración de claves públicas: autoridad certificante y certificados. Administración de claves de sesión compartidas. Seguridad de redes e Internet: Single Sign On, Infraestructura de Clave Pública PKI. Seguridad de WWW; comercio electrónico, gateways de pago, protocolo SET “Secure Electronic Transaction”; seguridad en IP IPSec: Firewalls, SSL. Seguridad en organizaciones: Firma Digital, Factura Electrónica; administración de identidades: identidades y cuentas directorio corporativo; gestión de identidades.

5. Documentación y proyectos de seguridad

Formulación y seguimiento de un Proyecto de Seguridad en base a un caso de estudio incluyendo el ciclo de vida de los sistemas de seguridad; fase inicial, fase de desarrollo y adquisición, fase de implementación, fase de operación y mantenimiento, fase de disposición.

6. Taller de Trabajo Final de Integración

Tipos de TF. Disposiciones individuales para el desarrollo del TF. Plan de trabajo para el desarrollo del TF. Criterios genéricos y normativos. Consideraciones acerca del plagio. Criterios de estilo de redacción y de citas académicas. Fuentes de información: búsqueda y selección. Reseñas bibliográficas. Tutorías grupales e individuales.

7. Seguridad en sistemas operativos y aplicaciones

Instalación y operación segura del sistema operativo. Ciclo de vida del desarrollo de sistemas. Desarrollo y gestión de bases de datos. Controles de los sistemas. Control en la operación y el mantenimiento de las aplicaciones. Aplicaciones distribuidas. Ataques y vulnerabilidades en aplicaciones y sistemas. Buffer Overflows, Format Strings, Race Conditions. Entornos protegidos (sandboxes, chroot). Mecanismos de protección: técnica del canario, segmento no ejecutable. Análisis de logs. HostIDS. Vulnerabilidades en web. Códigos maliciosos.

8. Comportamiento organizacional

Cultura organizacional. Clima organizacional. Comportamiento individual, grupal y organizacional. Dinámica de grupos. Valores y actitudes. Comunicación interpersonal. Motivación. Liderazgo. Trabajo en equipo. Resolución de conflictos. Negociación. Gestión del cambio organizacional. Inteligencias múltiples. El proceso de aprendizaje. Toma de decisiones individuales y grupales.

9. Seguridad en redes II

Problemas, amenazas, ataques, defensa y prevención: amenazas pasivas, ataques y códigos maliciosos; defensa y prevención, Intrusión Detection Systems Honeypots; análisis de vulnerabilidades, pruebas de penetración. Desarrollo seguro. Seguridad en Organizaciones: modelos de alta disponibilidad y seguridad; dominios de seguridad, monitoreo de seguridad; puntos de control. Ubicación de Firewalls, IDS.

10. Marco legal, ética y privacidad

Introducción al Derecho Informático, conceptos y terminología legal. Sistemas legales en Argentina y otros países. Régimen jurídico de protección de la Propiedad Intelectual. Régimen de Firma Digital. Ética y privacidad. Visión jurídica de lo delitos informáticos. Derecho Internacional: legislación transfrontera. Jurisprudencia.

11. Seguridad física

Administración y relevamiento de los riesgos. Planeamiento y gerenciamiento de la Seguridad Física. La tecnología y el diseño de procesos de trabajo. Aplicación de diseños. Sistemas de seguridad física.

12. Gestión estratégica de la seguridad II

Análisis y gestión del riesgo, modelo de valor, mapa de riesgos, evaluación de salvaguardas, informe de insuficiencias, catálogo de elementos, estado de riesgo. Ciclo de vida: análisis y gestión, planificación, implementación de salvaguardas, gestión de configuración y cambios. Relación y complementariedad entre los distintos estándares y/ modelos (frameworks), cumplimiento (compliance), regímenes e instituciones Internacionales y Nacionales: Cobit, Coso, BSI, ISO, ITIL, Basilea II, CMM, SOX, otros.

13. Criptografía II

Teoría de la información: entropía de Shannon. Entropía condicional. Transinformación. Distancia de unicidad. Algebra abstracta y sus aplicaciones criptográficas. Logaritmo discreto y ataques vinculados. Criptosistema ElGamal y ElGamal generalizado. Campos finitos GF(2^n) en criptosistemas simétricos (AES) y asimétricos (ElGamal). Máquinas de Turing y teoría de la complejidad computacional aplicadas a la criptología. Problemas complejos en campos numéricos. Algebra no conmutativa y aplicaciones criptográficas (GDH-Intercambio Diffie-Hellman generalizado y ZKP-Prueba de conocimiento cero). Curvas elípticas e hiperelípticas. Códigos lineales, problema de la mochila y otros. Ataque de criptoanálisis diferencial a las redes Feistel. Ataques de colisiones diferenciales a las funciones Hash. Estándar SHA3. Secretos compartidos y protocolos especiales (undeniable signatures, oblivious transfer, electronic cash) Secreto compartido. Elementos de criptografía cuántica, computación cuántica, teoría de información cuántica y sus aplicaciones criptográficas.

14. Auditoría

Control y auditoría. Normas técnicas. Control y estructura organizativa. Separación de funciones y oposición de intereses. Análisis específico del área de Seguridad Informática. Controles en las entradas al sistema y sus almacenamientos. Transacciones rechazadas y observadas. Concepto de monitoreo. Planificación de las actividades de auditoria. Pruebas de cumplimiento. Evaluación de aplicación de políticas, planes, normas, procedimientos, esquemas, estándares y métricas. Pruebas y técnicas asociadas. Pistas de auditoria. Evaluación del nivel de respuesta ante incidentes. Test de penetración. Test de nivel de divulgación y comprensión de políticas, normas y procedimientos en la organización. Comprobaciones y simulaciones sobre planes de contingencia, continuidad de operaciones y recuperación.

15. Informática forense y delitos informáticos

Análisis forense: objetivos, principios. Evidencia digital. Metodología de trabajo para el análisis de los datos: identificación de la evidencia digital, preservación del material informático, análisis de datos, presentación del dictamen pericial. Registros temporales. MACtimes. Registros de redes y DNS. File systems con journaling. File System: File System Virtual (VFS). Aspectos internos del File System. Estructura de una partición. Recolección de información volátil y no volátil. Recolección de evidencia de red. Análisis de archivos binarios: análisis estático y análisis dinámico. Consideraciones legales: evidencia y evidencia admisible. Obtención de evidencias. Tipos de evidencia. Características para ser admisible en juicio. Preservación de la cadena de custodia. Informes Periciales.

16. Taller de Desarrollo de Competencias Gerenciales

Desarrollo de casos y situaciones que permitan adquirir práctica en los siguientes aspectos: comunicaciones interpersonales, negociación, toma de decisiones, trabajo en equipo, liderazgo, motivación y gestión del cambio.

17. Taller de Trabajo Final de Maestría

Las actividades del Taller tienen como finalidad que garanticen el objetivo de realización del Trabajo Final de Maestría. Dichas actividades tienen su punto de apoyo en el tema del trabajo final, el cual, trabajado a lo largo de la cursada, irá tomando forma mediante la recolección de información y análisis realizados. El objetivo es que el maestrando tenga el apoyo necesario para presentar su proyecto y posterior trabajo.