Ciberseguridad

Carreras/Planes para los que se ofrece:

- Ingeniería en Informática – Plan 2006 implementación 2010.
- Se dicta en el 1er semestre.

Objetivos del curso

Brindar al estudiante los fundamentos conceptuales y técnicos del ciberespacio y la seguridad de la información, promoviendo la comprensión de modelos, marcos de referencia y metodologías básicas que permitan analizar escenarios de exposición, identificar vulnerabilidades y proponer medidas de mitigación en entornos organizacionales.

Temario del curso

1. Fundamentos y gestión de la seguridad de la información

1.1. Principios de seguridad: Confidencialidad, Integridad y Disponibilidad
1.2. Modelo Mc Cumber
1.3. Marcos de referencia: Marco de Ciberseguridad de AGESIC e ISO 27001 (visión estructural mínima)
1.4. Relación entre principios de seguridad y diseño técnico

2. Activos, exposición y reconocimiento

2.1 Activos desde la perspectiva técnica
2.2 Superficie de ataque interna y externa
2.3 Huella digital
2.1 Reconocimiento pasivo y OSINT técnico
2.2 Fuentes abiertas: WHOIS, DNS, motores de búsqueda avanzados
2.3 Enumeración pasiva de infraestructura: subdominios y certificados públicos
2.4 Análisis técnico de resultados
2.5 Análisis técnico de incidentes reales

3. Modelos de ataque y evaluación técnica

3.1 Modelos de ataque: Kill Chain y MITRE ATT&CK
3.2 Ciclo de ataque
3.3 Relación entre reconocimiento y explotación
3.4 Metodología básica de pentesting
3.5 Reconocimiento activo
3.6 Escaneo de puertos e identificación de servicios
3.7 Concepto de explotación controlada

4. Vulnerabilidades, hardening y seguridad técnica

4.1 Concepto técnico de vulnerabilidad
4.2 Lectura e interpretación de CVE
4.3 Análisis de impacto técnico
4.4 Ventana de exposición
4.5 Servicios expuestos y configuraciones inseguras

4.6 Arquitectura y riesgo
4.7 Gestión de usuarios y principio de mínimo privilegio
4.8 Permisos, servicios y superficie local de ataque
4.9 Hardening: configuraciones seguras, parches y reducción de superficie

5. Seguridad aplicada, criptografía y respuesta

5.1 Seguridad en aplicaciones
5.2 Errores frecuentes de validación
5.3 OWASP como marco conceptual
5.4 Vulnerabilidades web: SQL Injection, XSS y problemas de autenticación
5.5 Seguridad en APIs: control de acceso, autenticación y exposición de datos
5.6 Criptografía aplicada: hashing, contraseñas, criptografía simétrica y asimétrica
5.7 Comunicaciones seguras: TLS y certificados digitales
5.8 Errores frecuentes de implementación
5.9 Monitoreo, respuesta a incidentes e informe técnico

Evaluación y aprobación

- Mínimo de asistencia requerido: 50% del total de clases.
- Una prueba escrita individual (obligatoria) con un mínimo de aprobación de 50/100. o trabajo obligatorio grupal con Defensa, con un mínimo de aprobación de 50/100.
- Cumplidos los mínimos del régimen de evaluación, se aprueba la asignatura con una nota final en la escala de 6 a 12.
- En otro caso, se reprueba la asignatura con nota entre 1 y 5. Se podrá rendir examen en los períodos ordinarios (por el lapso de un año) siempre que se haya alcanzado el mínimo de asistencia requerido.

Docente

- Mag. Lic. Carlos Magallanes.