UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA
LICENCIATURA EN CIENCIAS INFORMATICAS
ENFASIS EN ANALISIS DE SISTEMAS INFORMATICOS
PLAN 2009
PROGRAMA DE ESTUDIOS

I. IDENTIFICACIÓN

1. Asignatura : Electiva II – Ciberseguridad
2. Grupo : Seis
3. Horas semanales : 5 horas
   - 3.1. Clases teóricas : 2 horas
   - 3.2. Clases prácticas : 3 horas
4. Total real de horas disponibles : 90 horas
   - 4.1. Clases teóricas : 36 horas
   - 4.2. Clases prácticas : 54 horas

II. JUSTIFICACIÓN

El despliegue de tecnología y conectividad ha puesto en un punto de interés la ciberseguridad. Esta área está en permanente análisis y evolución por parte de proveedores y desarrolladores de servicios, como las diversas áreas de las organizaciones y sus clientes. La ciberseguridad es tan amplia que abarca no solo aspectos técnicos, sino legales y culturales. Esta situación obliga a que los profesionales involucrados en áreas de tecnologías cuenten con aptitudes que les permitan incorporar criterios de ciberseguridad en cualquier tipo de emprendimiento que involucre tecnología. El curso se enfoca en incorporar los principios y fundamentos de la ciberseguridad a través de laboratorios y trabajos prácticos. Se da particular énfasis a la elaboración de trabajos de investigación aplicando metodologías de investigación.

III. OBJETIVOS

1. Definir los fundamentos y principios de la ciberseguridad.
2. Identificar los estándares de seguridad aplicables en las organizaciones.
3. Describir el ecosistema de Internet de las cosas, su gestión y desafíos de aplicación.
4. Definir los conceptos de defensa, herramientas de monitoreo y operación de políticas de seguridad en redes de computadoras.
5. Elaborar propuestas y soluciones a desafíos presentados en los seminarios.

IV. PRE - REQUISITO

- Base de Datos II
- Electiva I

V. CONTENIDO

5.1. Unidades programáticas

1. Fundamentos de la Ciberseguridad.
2. Principios de la Ciberseguridad.
3. Componentes de los Sistemas de Tecnologías de la Información.
4. Defensa en Redes de Computadoras.
5. Seguridad en Sistemas Operativos Modernos.
6. Seminarios sobre temas actualizados de Ciberseguridad.

5.2. Desarrollo de las unidades programáticas

1. Fundamentos de la Ciberseguridad.
   - 1.1. Amenazas y Adversidades.
   - 1.2. Vulnerabilidades y Gestión del Riesgo.
   - 1.3. Ataques comunes.
   - 1.4. Evaluación básica de Riesgos.
   - 1.5. Ciclo de Vida de la Seguridad.
   - 1.6. Aplicaciones de Criptografía y PKI.
   - 1.7. Seguridad de datos.
   - 1.8. Modelos de seguridad.
   - 1.9. Modelos de control de acceso.
   - 1.10. Confidencialidad, integridad, disponibilidad, acceso, autenticación, autorización, no repudio, privacidad.
   - 1.11. Gestión de sesión.
   - 1.12. Gestión de excepción.
   - 1.13. Mecanismos de seguridad.
   - 1.14. Detección de actividad maliciosa y formas de ataque.
   - 1.15. Contramedidas.
   - 1.16. Aspectos legales.

1.17. Ética asociada a la ciberseguridad.

2. Principios de la ciberseguridad.
   2.1. Separación
   2.2. Aislación
   2.3. Encapsulación
   2.4. Modularidad
   2.5. Simplicidad de diseño
   2.6. Minimizationofimplementation
   2.7. Diseño abierto
   2.8. Complete mediation
   2.9. Layering
   2.10. LeastPrivilege
   2.11. Falla segura
   2.12. LeastAstonishment
   2.13. Minimize Trust Surface
   2.14. Usabilidad
   2.15. Relaciones de confianza

3. Componentes de los sistemas de Tecnologías de Información
   3.1. Protección en los extremos. Estaciones de trabajo, servidores, appliances, dispositivos móviles, dispositivos periféricos.
   3.2. Dispositivos de almacenamiento.
   3.3. Arquitectura de Sistemas. Virtualización. Contenedores.Nube
   3.4. Ambientes alternativos. SCADA. Sistemas de tiempo real. Infraestructuras críticas.
   3.5. Redes de Computadoras. Internet. LAN. Inalámbrico.
   3.6. Mapeo de Redes de Computadoras. Enumeración e identificación de componentes de redes de computadoras.
   3.7. Componentes de Seguridad de Redes. Prevención de pérdida de datos. Redes Privadas Virtuales. Cortafuegos.
   3.8. Sistemas de Detección y Prevención de Intrusos. Respuesta de Incidentes.
   3.9. Servicios gestionados.
   3.10. Seguridad en software. Principios de codificación segura.
   3.11. Gestión de configuración.
   3.12. Parches. Actualizaciones de Sistemas Operativos y Aplicaciones.
   3.13. Exploración de vulnerabilidades.
   3.14. Seguridad y personas. Ingeniería social.
   3.15. Seguridad física y de ambiente.
   3.16. Internet de las Cosas.
   3.17. Asociaciones y colaboradores de la Ciberseguridad.

4. Defensa en las Redes de Computadoras
   4.1. Esquemas de defensa de red. Defensa en profundidad. Ataques de red. Hardening. Exposición minimizada.
   4.2. Herramientas de Monitoreo y Defensa de Red. Cortafuegos. DMZ. Servidores Proxy.VPN. Honeypots y Honeynets. IDS/IPS
   4.3. Operaciones de Red. Monitoreo de Seguridad de Red. Análisis de tráfico de red
   4.4. Políticas de seguridad de red. Control de acceso a la red. Desarrollo y aplicación de Políticas de red.

5. Seguridad en Sistemas Operativos Modernos.
   5.1. Estados privilegiados y no privilegiados.
   5.2. Procesos e hilos de aplicaciones.
   5.3. Memoria
   5.4. Sistemas de archivos
   5.5. Virtualización. Hipervisores.
   5.6. Creación y operación de tecnología de virtualización.
   5.7. Principios fundamentales de diseño de seguridad aplicados a un sistema operativo.
   5.8. Controles de Acceso.
   5.9. Separación de dominios, aislamiento de procesos, encapsulación de recursos, disminuir privilegios.

6. Seminarios sobre temas actualizados en Ciberseguridad.

VI. ESTRATEGIAS METODOLÓGICAS

1. Las clases teóricas se desarrollan con apoyo de medios audiovisuales.
2. Las prácticas de laboratorio y trabajos prácticos con guías preparadas por el docente.
3. Lecturas previas a las clases de temas determinados, por los estudiantes
4. Participarán en seminarios relacionados al área de la asignatura.
5. Técnicas grupales e individuales para realización de trabajos.
6. Presentación y defensa de trabajos de investigación y de artículos científicos relacionados con el área.
7. Evaluación continua

VII. MEDIOS AUXILIARES

1. Equipo multimedia
2. Pizarra
3. Marcadores
4. Borrador de pizarra
5. Equipamiento de laboratorio

6. Herramientas de virtualización y simulación

VIII. EVALUACIÓN

Para la evaluación de la asignatura se tendrá en cuenta lo siguiente:

1. Laboratorios, trabajos prácticos y de investigación.
2. Es imprescindible el desarrollo de los laboratorios, la entrega de todos los trabajos prácticos y la asistencia a los seminarios**.**
3. Las calificaciones se basan en el Reglamento y Normativas de la Facultad Politécnica.

IX. BIBLIOGRAFÍA

A. Básica

- ISO/IEC 27001. (2013). Information Security Management.
- National Institute of Standards and Technology. (2018). Cybersecurity Framework. Version 1.1.

B. Complementaria

- Abolhassan, F. (2017). *Cyber Security*. Simply. Make it Happen. Leveraging digitization through IT security. Springer International Publishing AG.
- Ackerman, P. (2017). *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*. Packt Publishing Ltd. Birmingham.
- Hertzog, R. (2017). *Kali Linux Revealed: Mastering the Penetration Testing Distribution*. Offsec Press. Cornelius NC.
- Russell, B. (2016). *Practical Internet of Things Security*. A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world. Birmingham.
- Salmon, A. (2017). *Applied Network Security*. Master the art of detecting and averting advanced network security attacks and techniques. Birmingham.

COLECCIÓN DE LA BIBLIOTECA DE LA FACULTAD POLITÉCNICA

- Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. (2011). Madrid: Ministerio de Defensa.

BASE DE DATOS ON LINE

- Metcalf, L., & Casey, W. (2016). Cybersecurity and applied mathematics. Cambridge, MA: Syngress is an imprint of Elsevier. Disponible en: CICCO Conacyt Paraguay
- IEEE Cybersecurity Development Conference (1°: 2016: Boston, Mass.), IEEE Cybersecurity Initiative, IEEE Computer Society, & Institute of Electrical and Electronics Engineers. (2016). *2016 ieee cybersecurity development: Proceedings: 3-4 november 2016, boston, massachusetts*. Los Alamitos, California: Conference Publishing Services, IEEE Computer Society. Disponible en: CICCO Conacyt Paraguay
- Bartiss, M., Menke, A., & Paluzzi, D. (2018). Cybersecurity and cyberliability. *Journal of Aapos, 22*(4), 86. doi:10.1016/j.jaapos.2018.07.318