FACULTAD DE INFORMÁTICA | UNIVERSIDAD NACIONAL DE LA PLATA

SEGURIDAD Y PRIVACIDAD EN REDES Año 2020	**Carrera:** Maestría en Redes de Datos **Docentes Responsables:** Lic. Javier Díaz Lic. Paula Venosa Mg. Nicolás Macia **Duración:** 120 hs.

OBJETIVOS GENERALES:

Comprender conceptos básicos relacionados a la seguridad de la información Analizar distintas herramientas para comprender riegos existentes y analizar la seguridad en la organización Estudiar normas, mecanismos y protocolos para proteger las redes y sus aplicaciones.

CONTENIDOS MINIMOS:

- Conceptos básicos de seguridad y terminología relacionada.
- Gestión de seguridad de la información, en el marco de las normas ISO 27001 e ISO 27002
- Legislación nacional relacionada a seguridad de la información.
- Amenazas: Técnicas de descubrimiento, scanning, sniffing, etc.
- Criptografía y sus aplicaciones (Firma digital, PGP, Esteganografía).
- Vulnerabilidades de los sistemas - Ataques. Seguridad de aplicaciones WEB.
- Mecanismos de protección: Firewalls, IDS e IPS y honeypots.

PROGRAMA

Unidad I: Introducción

Seguridad y Privacidad - Conceptos básicos de seguridad - Atributos de seguridad: confidencialidad, integridad, autenticidad, no repudio - Vulnerabilidad, Amenaza, Incidente- Tipos de amenazas – Ejemplos. Seguridad Física.

Unidad 2: Gestión de seguridad de la información

Definiciones - ISO 27000: Generalidades de la serie - ISO 27001: Ciclo de gestión de la seguridad de la información - Objetivos de control e implementación de controles - Aspectos claves de un SGSI

Unidad 3: Descubrimiento
Técnicas de descubrimiento: Footprinting - Fingerprinting de SO y de servicios - Escaneo y técnicas de escaneo basadas en TCP y UDP - Herramientas de escaneo y análisis

Unidad 4: Sniffing
Conceptos básicos de sniffing - Técnicas de sniffing en redes switcheadas - Herramientas - Técnicas de detección de sniffing - Análisis de muestras de tráfico

Unidad 5: Criptografía
Definiciones - Historia - Criptografía Simétrica - Criptografía Asimétrica - Aplicaciones de la criptografía: Infraestructuras de clave pública - PGP - Firma Digital: Aspectos técnicos y legales -Uso de la criptografía en los servicios WWW, correo electrónico - Esteganografía

Unidad 6: Mecanismos de protección
Firewalls - Políticas de filtrado - Reglas de filtrado - Sistemas de detección de intrusiones (IDS) - Tipos de IDS - Sistemas de prevención de intrusiones - Tipos de IPS - Honeypots - Herramientas

ACTIVIDADES EXPERIMENTALES y DE INVESTIGACION

Tareas en Laboratorio

Todas las unidades incluyen el desarrollo de prácticas: las unidades 1 y 2 son trabajos de elaboración personal y en grupo, de aplicación de los conceptos y de presentación de propuestas y análisis de los alumnos en el marco de la organización donde trabajan.
En las siguientes unidades se realizan actividades de laboratorio en entornos virtuales provistos por la cátedra, con herramientas opensource ampliamente utilizadas, para desarrollar las temáticas de Descubrimiento, Sniffing, Criptografía y Mecanismos de Protección.

Investigación:

Los alumnos analizan reportes de seguridad, estudian normas y artículos relacionados con los diferentes temas abordados en el curso, provistos por los docentes, a fin de aprender las temáticas de las distintas unidades en forma integral teniendo en cuenta el contexto en el cual funcionan las organizaciones, las redes y los sistemas.
También se referencian numerosas herramientas en complemento a las que se utilizan, de manera de despertar la curiosidad y dar la posibilidad a la investigación autónoma por parte de los alumnos, con el objetivo de enriquecerlos e iniciar en quienes no posean esa práctica desde lo profesional, el contacto con el proceso de investigación y poder desarrollar interés en temas a considerar en su propuesta de tesis.

METODOLOGIA DE EVALUACION

La materia se aprueba con actividades de seguimiento durante la cursada (entregas o evaluaciones online de cada unidad) y una evaluación al final del curso. Según el resultado de la evaluación final podrá completarse la misma con un coloquio. Para aquellos que no hayan aprobado se contempla una recuperación.

BIBLIOGRAFIA

- Network security assessment Chris McNab O'Reilly 3rd ed. 2017. ISBN-13: 978-1491910955; ISBN-10: 149191095X
- Cryptography and network security: principles and practice, Stallings, William 8th ed.2017. ISBN-13: 978-0134444284; ISBN-10: 0134444280X
- CISSP certification exam guide Harris, Shon, McGraw-Hill Osborne Media; 2nd ed. 2003. ISBN-10: 0072230908; ISBN-13: 978-0072230901
- OWASP Testing Guide OWASP Foundation. Creative Commons Attribution-ShareAlike 4.0.
- http:/ha.ckers.org/xss.html
  http:/www.cert.org/tech_tips/malicious_code_mitigation.html
  http:/www.w3schools.com/HTML/html_entities.asp
  http:/www.iss.net/security_center/advice/Intrusions/2000639/default.htm
  http:/www.joelonsoftware.com/articles/Unicode.html