FACULTAD DE INFORMÁTICA

UNIVERSIDAD NACIONAL DE LA PLATA

SEMINARIO TÉCNICO SEGURIDAD TENDENCIAS EN GESTIÓN Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD INFORMÁTICA Año 2020	**Carrera:** Maestría en Redes de Datos **Docentes Responsables:** Lic. Javier Díaz Dr. Darío Piccirilli **Duración:** 40 hs.

OBJETIVOS GENERALES:

Completar la formación en análisis y detección de posibles ataques y gestión de los mismos, completando un enfoque técnico y gerencial, dando a conocer estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles incidentes de seguridad a la infraestructura o a la información.

CONTENIDOS MINIMOS:

Introducción y Conceptos
Estándares y buenas prácticas
Tendencias en ataques
Infraestructuras críticas
Computer Incident Response Teams(CIRT)
Fuga de datos

PROGRAMA:

Módulo 1: Introducción y conceptos
Sobre este curso
Concepto de ciberseguridad y relacionados
Conceptos relacionados al riesgo: vulnerabilidades, amenazas, probabilidad e impacto.
Sistemas de Gestión de la Seguridad.
El valor de la información en la organización

Módulo 2: Estándares y buenas prácticas
Gestión del Riesgo. Estándares asociados

El Programa Cybersecurity Nexus (CSX) de ISACA
Global Cybersecurity Index (ITU)

Módulo 3: Tendencias en ataques.
Problemas de seguridad actuales:
Seguridad en dispositivos móviles.
BYOD / BYOT
Phishing
Malware / Botnet
DOS / DDOS

Módulo 4: Infraestructuras críticas
Concepto de criticidad
Determinación de lo crítico. Metodologías
National Cybersecurity Strategy (NCS), ITU
Cybersecurity Information Exchange Techniques (CYBEX), ITU.

Módulo 5: Computer Incident Response Teams (CIRT)
Concepto. Qué es un CIRT.
Gestión de Incidentes.
Caso: CIRTUNLP

Módulo 6:
1er parte: Fuga de datos (data leaks)
Consecuencias.
Tecnologías Data Leakage Prevention (DPL)
Estados de la información.
Sanatización de dispositivos
2da parte: Pautas de concientización en Ciberseguridad
Distintas experiencias

ACTIVIDADES EXPERIMENTALES y DE INVESTIGACION

Los temas se presentan mediante exposiciones de los instructores y la puesta en práctica de los conceptos a través de ejemplos, y fundamentalmente con el análisis de casos de estudio aprovechando la experiencia profesional de los docentes en el tema.
También se trabaja sobre material de lectura propuesto para determinados temas fundamentalmente para facilitarles el proceso de elección del tema de investigación para el trabajo de tesis. Motivo por el cual se provee una extensa bibliografía.

METODOLOGIA DE EVALUACION

Al finalizar el curso se deberán presentar y aprobar un informe individual de análisis y diagnóstico de casos de incidentes.

BIBLIOGRAFÍA

- https://www.ccn-cert.cni.es/publico/dmpublidocments/CCNCERT_IA-03-14-Ciberamenazas_2013_Tendencias_2014-publico.pdf
- CCN-STIC-450 Seguridad en dispositivos móviles. May. 2013
- CCN-STIC-457 Herramienta de gestión de dispositivos móviles: MDMNov. 2013
- “Critical Capabilities for Mobile Device Management Software”.Gartner.May 23, 2013. ID: G00250008
- Hunt, Edward (2012). "US Government Computer Penetration Programs and the Implications for Cyberwar", IEEE Annals of the History of Computing 34(3)
- Long, Johnny (2007). Google Hacking for Penetration Testers, Elsevier
- ISACA. Implementing the NIST Cybersecurity Framework (CSX).
- ISO/IEC 27001 Y 27005
- National Institute of Standards and Technology (NIST). NIST Special Publication 800-39
- ISACA. Prevención en Fuga de Datos. 2010
- National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1. January 10, 2017
- National Institute of Standards and Technology (NIST). NIST Special Publication 800-88. Guidelines for Media Sanitization
- Nassim Nicholas Taleb. El cisne Negro. El impacto de lo altamente improbable, 2a. Ed. Ediciones Paidós, 2010