FACULTAD DE INFORMÁTICA | UNIVERSIDAD NACIONAL DE LA PLATA

CONCEPTOS AVANZADOS DE SEGURIDAD INFORMATICA **Año 2018**	**Carrera:** Doctorado en Ciencias Informáticas **Docente Responsable:** Lic. Javier Díaz – Lic. Paula Venosa – Mg. Nicolás Macia **Créditos: 4** **Duración**: 70 horas

OBJETIVOS GENERALES

Este curso tiene como objetivo brindar al alumno conceptos de Seguridad avanzados, relacionados a las tendencias actuales en la materia.
El curso tiene como objetivo que el alumno comprenda los aspectos técnicos relacionados a amenazas de seguridad existentes hoy en día en las redes y aplicaciones de las organizaciones, y los mecanismos de mitigación que pueden implementarse a fin de minimizar los riesgos que dichas amenazas provocan.
También se espera que el alumno se familiarice con los servicios básicos que binda un CSIRT, a través de ejemplos concretos y ejercitación afin.
Se espera motivar al alumno presentando líneas de trabajo e investigación en el área y brindando un panorama a partir del cual pueda elegir áreas donde continuar especializándose para aplicar sus conocimientos en el ámbito de su desarrollo profesional y de su formación académica.

MODALIDAD DE EVALUACION

La aprobación del mismo consistirá en la realización de los ejercicios prácticos que se presenten durante el curso y una entrega derivada de la práctica.

CONTENIDOS MÍNIMOS

Unidad 1:
Tendencias en ataques hacia los usuarios: phishing, malware, spam, etc. Tendencias en ataques hacia las redes, los servicios y las aplicaciones WEB. Nuevas tendencias: Hacking as a service, data leak, cloud computing. Botnets: conceptos básicos y prácticos relacionados a su funcionamiento.

Unidad 2:
Mecanismos de protección del usuario: Concientización, buenas prácticas en la navegación y en el uso de dispositivos móviles, privacidad y anonimato. Mecanismos de protección de la infraestructura: Firewalls, sistemas de detección de intrusiones (IDS de host, IDS de red y IDS de filesystem). Web Application Firewall.

Unidad 3:
CSIRTs. Servicios brindados por el mismo: servicios proactivos, reactivos y de gestión de calidad de la seguridad. Descripción detallada del proceso de atención de incidentes. Metodología de trabajo en un CSIRTs y herramientas de soporte. Pentest. Monitoreo de seguridad. Estándares para nomenclatura de vulnerabilidades de seguridad.

BIBLIOGRAFÍA

1. http://www.antiphishing.org/resources/mobile/
2. http://www.trendmicro.com/vinfo/us/security/threat-intelligence-center/
3. http://www.thoughtcrime.org/software/sslstrip/
4. https://www.openssl.org/~bodo/ssl-poodle.pdf
5. http://heartbleed.com/
6. http://www.owasp.org
7. https://www.honeynet.org/papers/bots/
8. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html
9. Botnets: Detection, Measurement, Disinfection & Defence – Enisa
10. A Review on IRC Botnet Detection and Defence - Bernhard Waldecker
11. https://datatracker.ietf.org/doc/rfc2979/
12. www.netfilter.org/
13. http://www.faqs.org/docs/iptables/
14. http://www.snort.org
15. http://sourceforge.net/projects/tripwire/
16. www.fail2ban.org/
17. http://www.first.org/
18. http://www.lacnic.net/web/lacnic/ipv6
19. Manual Gestión de Incidentes de Seguridad Informática – Proyecto Amparo (http://www.proyectoamparo.net/files/manual_seguridad/manual_basico_sp.pdf)
20. http://www.mitre.org