Ministerio de Cultura y Educación **(Programa del año 2019)**
Universidad Nacional de San Luis **(Programa en trámite de aprobación)**
Facultad de Ciencias Físico Matemáticas y Naturales **(Presentado el 25/11/2019 15:26:19)**
Departamento: Informatica
Area: Area II: Sistemas de Computacion

I - Oferta Académica

Materia	Carrera	Plan	Año	Período
(OPTATIVAS) CIBERSEGURIDAD	TEC.REDES COMP.	12/15	2019	2° cuatrimestre

II - Equipo Docente

Docente	Función	Cargo	Dedicación
CASTRO, ALICIA DOMINGA MERCE	Responsable de Práctico	JTP Exc	40 Hs

III - Características del Curso

Credito Horario Semanal				
Teórico/Práctico	**Teóricas**	**Prácticas de Aula**	**Práct. de lab/ camp/ Resid/ PIP, etc.**	**Total**
4 Hs	Hs	Hs	2 Hs	6 Hs

Tipificación	Periodo
B - Teoria con prácticas de aula y laboratorio	2º Cuatrimestre

Duración			
Desde	**Hasta**	**Cantidad de Semanas**	**Cantidad de Horas**
05/08/2019	16/11/2019	15	90

IV - Fundamentación

Los ciberataques evolucionan con gran rapidez. En la actualidad existen numerosas y variadas amenazas que incluye actores individuales o grupos que generan ataques a sistemas para obtener información datos o afectar la disponibilidad de los mismos perjudicando el negocio y reputación de las empresas u organismos.
Es de principal prioridad que los profesionales informáticos conozcan las amenazas, vulnerabilidades que afectan a los activos de información, seleccionar técnicas y mecanismos para defender y proteger los equipos informáticos (computadoras, servidores, dispositivos móviles), los sistemas de comunicación y principalmente los datos almacenados y en transito de ataques maliciosos, así también conozcan buenas prácticas para el desarrollo seguro de aplicaciones web.

V - Objetivos / Resultados de Aprendizaje

Concientizar en los problemas asociados a ciberseguridad.
Desarrollar la habilidad para identificar amenazas y vulnerabilidades de los activos de información.
Informar sobre la legislación dirigida a la protección de la información.
Analizar riesgos relacionados con la seguridad de la información
Desarrollar la habilidad de elección de mecanismos de protección y mitigación de riesgos de los activos de información frente a ciberataques.
Aprender a desplegar campañas de concientización y capacitación.
Conocer las amenazas y vulnerabilidades a las que está expuestas las aplicaciones web y las bases de datos.
Identificar contramedidas necesarias para aumentar la seguridad en las aplicaciones web, desde el código hasta la infraestructura web.

VI - Contenidos

Unidad 1. Introducción y conceptos básicos.
Ciberseguridad, seguridad de la información. Estado actual de la ciberseguridad. Ciberresilencia. Estrategias de seguridad informática. Áreas de trabajo en SI. Etapas de SI. Amenazas, vulnerabilidades, servicios de SI, ataques. Análisis de casos reales

Unidad 2. Arquitectura de Seguridad
Normativas. Política de Seguridad. Infraestructura Tecnológica. Estructura de organización de Seguridad de Información. Campañas de concientización y capacitación.

Unidad N°3. Seguridad en redes y Cloud
Identificación de activos, amenazas, vulnerabilidades y ataques en una red LAN y en el Cloud. Herramientas de reconocimiento de la red: escaneo de puertos. Técnicas de mitigación: cifrado, certificados digitales, VPN, almacenamiento seguro, administración y monitoreo, DMZ. Recomendaciones en el uso de Cloud.

Unidad N°4. Seguridad en aplicaciones Web y Base de datos
Identificación de amenazas y tipos de ataques en aplicaciones web y bases de datos. Análisis de vulnerabilidades. OWASP. Recomendaciones en el desarrollo seguro de aplicaciones web.

Unidad N°5. Seguridad en dispositivos Móviles
Identificación de vulnerabilidades, activos, amenazas, tipos de ataque en dispositivos móviles. Identificación de seguridad aplicada por los stores de apps. Recomendaciones en el uso e instalación de apps en dispositivos móviles.

VII - Plan de Trabajos Prácticos

Cada unidad tendrá un trabajo practico conformado por preguntas de razonamiento teórico e investigativo y actividades de laboratorio, con resolución de desafíos semanales incrementales. Cada desafío consiste en resolver un problema, según el avance del tema dado.
Las actividades de laboratorio, se trabajarán con maquinas virtualizadas completamente configuradas. Algunas disponen de herramientas para evaluar la seguridad, otras son maquinas con aplicaciones web vulnerables, entregadas por la cátedra

Trabajo Practico N.º 1. Introducción y conceptos básicos
Laboratorio N.º 1. Creación de laboratorio.
Trabajo Practico N.º 2. Arquitectura de Seguridad
Laboratorio N.º 2. Uso de Gestor de contraseñas
Trabajo Practico N.º 3. Seguridad en redes
Laboratorio N.º 3. Uso de criptografia en email
Laboratorio N.º 4. Obtener información de la red
Laboratorio N.º 4. Crear certificados digitales para HTTPS
Trabajo Practico N.º4. Seguridad Web
Laboratorio N.º 6. Análisis de vulnerabilidades web.
Trabajo Practico N.º 5. Seguridad Móvil y Seguridad en la nube

VIII - Regimen de Aprobación

Las condiciones para:
Para la obtención de la regularidad, el alumno debe:
1) Tener aprobada la carpeta de Trabajos Prácticos de acuerdo a las modalidades de presentación que se indique. Se hará énfasis en el cumplimiento de las fechas de presentación.
2) Aprobar con 4 (cuatro) una evaluación. La cual tiene dos instancias de recuperación según OCS 32-14.
3) Presentar un informe con exposición de un caso de estudio.

Para la aprobación de la materia, el alumno puede optar por:
1. Promoción Directa
2. Por regularización y examen final

1.Promoción Directa:
Tener aprobada la carpeta de Trabajos Prácticos. Se hará énfasis en el cumplimiento de las fechas de presentación.
Aprobar con 7 (siete) la evaluación. La cual tiene dos instancias de recuperación según OCS 32-14.
Presentar un informe con exposición de un caso de estudio.
Rendir una evaluación final integradora.
Tener un 80% de asistencia.

2. Por regularización. Aprobando un examen final Teórico/ Práctico en mesa de examen definida en calendario académico.

IX - Bibliografía Básica

[1] Fundamentos De Seguridad En Redes. Aplicaciones Y Estándares. 2° Edición. William Stallings. 2003
[2] Building Internet Firewalls. Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman. Second Edition, June 2000
[3] Web Security Testing Cookbook. O'Reilly. Paco Hope and Ben Walther. 2009
[4] Glosario de terminos de Ciberseguridad. Incibe. 2017
[5] OWASP Top 10. OWASP.org. 2017 https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf
[6] Information Security Architecture. An Integrated Approach to Security in the Organization. Second Edition. Jan Killmeyer. 2006
[7] Ley 25.326. Ley argentina sobre Protección de Datos Personales
[8] Seguridad de Dispositivos Móviles: Android 7.x . Centro Criptológico Nacional Español, 2018

X - Bibliografia Complementaria

[1] Cloud Security and Privacy. Tim Mather, Subra Kumaraswamy, and Shahed Latif. 2009. O'Really
[2] The Basics of Hacking and Penetration Testing. Ethical Hacking and Penetration Testing Made Easy. Patrick Engebretson. Elsevier. 2011
[3] Guía para proteger y usar de forma segura su móvil. Instituto Nacional de Tecnologías de la Comunicación de España (INTECO), www.inteco.es

XI - Resumen de Objetivos

Concientizar en los problemas asociados a ciberseguridad.
Desarrollar la habilidad para identificar amenazas y vulnerabilidades de los activos de información, infraestructuras y aplicaciones web.
Analizar riesgos relacionados con la seguridad de la información
Desarrollar la habilidad de elección de mecanismos de protección y mitigación de riesgos de los activos de información, implementación y desarrollo de aplicaciones web seguras.
Aprender a desplegar campañas de concientización y capacitación.

XII - Resumen del Programa

Unidad N° 1. Introducción y conceptos básicos
Unidad N° 2. Arquitectura de Seguridad
Unidad N° 3. Seguridad en redes y Cloud
Unidad N° 4. Seguridad en aplicaciones Web y Base de datos
Unidad N° 5. Seguridad en dispositivos Móviles

XIII - Imprevistos

XIV - Otros

ELEVACIÓN y APROBACIÓN DE ESTE PROGRAMA	
	Profesor Responsable
Firma:	
Aclaración:	
Fecha:	