Ministerio de Cultura y Educación **(Programa del año 2021)**
Universidad Nacional de San Luis **(Programa en trámite de aprobación)**
Facultad de Ciencias Físico Matemáticas y Naturales **(Presentado el 01/12/2021 18:58:08)**
Departamento: Informatica
Area: Area II: Sistemas de Computacion

I - Oferta Académica

Materia	Carrera	Plan	Año	Período
(ELECTIVA I) E.I.(CIBERSEGURIDAD)	PROF.CS.COMPUT.	06/09	2021	2° cuatrimestre

II - Equipo Docente

Docente	Función	Cargo	Dedicación
CASTRO, ALICIA DOMINGA MERCE	Prof. Responsable	P.Adj Exc	40 Hs

III - Características del Curso

Credito Horario Semanal				
Teórico/Práctico	**Teóricas**	**Prácticas de Aula**	**Práct. de lab/ camp/ Resid/ PIP, etc.**	**Total**
Hs	4 Hs	3 Hs	1 Hs	8 Hs

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

Duración			
Desde	**Hasta**	**Cantidad de Semanas**	**Cantidad de Horas**
23/08/2021	26/11/2021	14	118

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 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 y 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, como la importancia de aplicar buenas prácticas para el desarrollo seguro de aplicaciones web y móviles.

V - Objetivos / Resultados de Aprendizaje

Concientizar en los problemas asociados a ciberseguridad.
Desarrollar la habilidad para identificar amenazas y vulnerabilidad 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. Áreas de trabajo en SI. Etapas de SI. Amenazas, vulnerabilidades, servicios de SI, ataques, ciclo de vida de un ataque, análisis de ataques reales. Vectores de ataque: Malware, SPAM, Phising, botnet.

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, inalámbricas y en el Cloud. Herramientas de reconocimiento de la red: escaneo de puertos. Técnicas de mitigación: cifrado: certificados digitales, VPN; DMZ: Firewall, VLAN, ACL; almacenamiento seguro, administración y monitoreo.

Unidad N°4. Seguridad en aplicaciones Web, Móviles y Base de datos
Identificación de amenazas y tipos de ataques en aplicaciones web, móviles y bases de datos. Análisis de vulnerabilidades. OWASP. Recomendaciones en el desarrollo seguro de aplicaciones web (S-SDLC). 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

Trabajo Práctico N.º 1. Introducción y conceptos básicos
Trabajo Práctico N.º 2. Arquitectura de Seguridad
Trabajo Práctico N.º 3. Campaña de concientización o capacitación
Trabajo Práctico N.º 4. Seguridad en redes y Cloud
Trabajo Práctico N.º 5. Seguridad en Aplicaciones Web y Base de datos
Trabajo Práctico N.º 6. Seguridad Móvil

Laboratorio N.º 1. Creación de laboratorio virtualizado
Laboratorio N.º 2. Cifrado: Simétrico y HTTPS
Laboratorio N.º 3. Análisis de vulnerabilidades web.

Se acompañara con actividades en el campus virtual: foros, wiki, etc.

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.

Para la aprobación de la materia, el alumno puede optar por:
1. Promoción Directa
2. regularizando y rindiendo un 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 nota igual o superior a 7 (siete) la evaluación o sus recuperaciones. La cual tiene dos instancias de recuperación según OCS 32-14.
Tener como mínimo un 80% de asistencia.
Participación continua en actividades en campus virtual.

Aprobar una evaluación final integradora con nota igual o superior a 7 (siete).
2. Por regularización. Obteniendo la regularidad según lo indicado anteriormente y probando 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] Enciclopedia de la Seguridad Informática. 2° ED. Alvaro Gomez Vieites. Ra-Ma. 2011
[3] Building Internet Firewalls. Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman. Second Edition, June 2000
[4] Web Security Testing Cookbook. O'Reilly. 2009. Paco Hope and Ben Walther
[5] Glosario de terminos de Ciberseguridad. Incibe. 2017
[6] OWASP Top 10. OWASP.
[7] Information Security Architecture. An Integrated Approach to Security in the Organization. Second Edition. Jan Killmeyer. 2006
[8] Ley 25.326. Ley Argentina sobre Protección de Datos Personales
[9] Seguridad de Dispositivos Móviles: Android 7.x . Centro Criptológico Nacional Español, 2018
[10] Una Guía para Construir Aplicaciones y Servicios Web Seguros. 2005. OWASP
[11] OWASP TESTING GUIDE. 2008. OWASP

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 y aplicaciones web.
Informar sobre la legislación dirigida a la protección de la información.
Desarrollar la habilidad de elección de mecanismos de protección y mitigación de riesgos de los activos de información, aplicaciones web y bases de datos.
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, Móvil y Base de datos

XIII - Imprevistos

Según Resolución 1404 el Segundo Cuatrimestre de 2021 posee 14 semanas. A los efectos de que se impartan todos los contenidos y se respete el crédito horario establecido en el Plan de estudios de la carrera para la asignatura, se establece que se de cómo máximo 8 hs por semana distribuidas en teorías, prácticos y consultas, hasta completar las 100hs.

XIV - Otros

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