Ministerio de Cultura y Educación **(Programa del año 2024)**
Universidad Nacional de San Luis
Facultad de Ciencias Físico Matemáticas y Naturales
Departamento: Informatica
Area: Area II: Sistemas de Computacion

I - Oferta Académica

Materia	Carrera	Plan	Año	Período
() CIBERSEGURIDAD	ING. EN COMPUT.	28/12026/1	2024	2° cuatrimestre
() CIBERSEGURIDAD	ING. INFORM.	2-08/15	2024	2° cuatrimestre
() CIBERSEGURIDAD	LIC.CS.COMP.	32/12	2024	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**
5 Hs	Hs	Hs	Hs	5 Hs

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

Duración			
Desde	**Hasta**	**Cantidad de Semanas**	**Cantidad de Horas**
05/08/2024	15/11/2024	15	75

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

V - Objetivos / Resultados de Aprendizaje

Los objetivos de la actividad curricular son los siguientes:

- Concientizar en los problemas asociados a la seguridad de la información.
- 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 están 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. Activos de información, Estado actual de la ciberseguridad. Amenazas, vulnerabilidades, dimensiones de Seguridad de la Información: Integridad, disponibilidad y Confidencialidad, privacidad, incidentes, ciberataques: tipos, ciclo de vida de un ataque, análisis de ataques reales. Vectores de ataque: Malware, SPAM, botnet. Ingeniería social.

Unidad N°2. Seguridad en el desarrollo de sofware
Seguridad en el desarrollo de los Sistemas de Información. Identificación de amenazas y tipos de ataques en las aplicaciones. Legislaciones de protección de datos personales, crediticios y de salud. Ciclo de vida del desarrollo seguro de aplicaciones (S-SDLC). Herramientas de testing en el desarrollo de aplicaciones. Mecanismos de protección en el desarrollo de software: cifrado, control de acceso: autenticación, autorización, hash, validación de entradas, etc.

Unidad N°3. Seguridad en aplicaciones Web, Móviles y Base de datos
Seguridad de Sistemas de Información asociados a 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 web. OWASP. Mecanismos de mitigación en el desarrollo de aplicaciones web y protección a la bases de datos: Integridad, disponibilidad, autenticación, autorización, anonimización.

Unidad N°4. Seguridad en redes y Cloud
Seguridad en sistemas de información en particular en la infraestructura de red 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 protección: control de acceso, redundancia

VII - Plan de Trabajos Prácticos

Metodología de enseñanza
Por cada unidad se deja disponible el material correspondiente a los contenidos de la unidad: presentación, apunte teórico y su correspondiente trabajo práctico en el repositorio digital.
Para una mejor organización, los estudiantes tendrán a su disposición el cronograma con la descripción de las actividades que se realizan cada día de clase.
Los trabajos prácticos correspondientes a las unidades temáticas del programa consisten en problemas desafiantes que deben ser resueltos por los estudiantes guiados por los docentes.
Los trabajos prácticos incluyen actividades teóricas con consulta bibliográfica y actividades de razonamiento utilizando casos o situaciones. La consulta bibliográfica busca incentivar a la continua lectura y actualización de conocimientos en distintas fuentes bibliográficas no solo libros, sino web especializadas en la temática. El razonamiento práctico no solo permite la interrelación de los conceptos dados sino busca fortalecer el debate, generar comunicación efectiva con su correspondiente reflexión, evaluando e incentivando a la ética y responsabilidad del profesional informático, el impacto de las acciones en la sociedad y el trabajo en equipo de forma colaborativa y activa.
Se acompaña la actividad utilizando herramientas digitales que permiten resolución de las actividades solicitadas utilizando cuestionarios con multiple choice, relación de conceptos, y foros de partición conjunta. Con esta actividad se pretende que el alumno desarrolle capacidades de redacción, uso del vocabulario correcto y permite al docente detectar conceptos no asimilados.
Con el objetivo de realizar una evaluación formativa y continua, en cada trabajo práctico se solicita la entrega de ciertos ejercicios, permitiendo al alumno medir su nivel de apropiación del conocimiento y al docente tomar decisiones sobre el avance del proceso de enseñanza/aprendizaje para reforzar los conceptos en caso necesario o modificar la didáctica empleada, antes de llegar a las instancias evaluativas.
Los estudiantes podrán asistir a consulta para aclarar dudas que surjan con los ejercicios prácticos permitiendo también el acercamiento entre los estudiantes y los docentes.

Trabajos Prácticos
Trabajo Practico N.º 1. Conceptos básicos. Ataques
Trabajo Practico N.º 2. Ingeniería social. Campañas de Capacitación. Políticas de seguridad.
Trabajo Practico N.º 3. Vulnerabilidad
Trabajo Practico N.º 4. Confidencialidad e integridad
Trabajo Practico N.º 5. Control de acceso y disponibilidad
Trabajo Practico N.º 6. Ciclo de vida del desarrollo del software seguro
Trabajo Practico N.º 7. Seguridad en infraestructura

Laboratorios
Laboratorio: Instalación de administrador de contraseñas.
Laboratorio. Análisis de vulnerabilidades web
Laboratorio. Obtener información de la red
Laboratorio: Cifrado de archivos

Trabajo Practico integrador

VIII - Regimen de Aprobación

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

1.Promoción Directa:
Tener aprobados los Trabajos Prácticos solicitados. Se hará énfasis en el cumplimiento de las fechas de presentación.
Aprobar con nota igual o superior a 7 (siete) la evaluación o alguna de sus dos recuperaciones, según lo establece la normativa vigente.
Tener como mínimo un 80% de asistencia, la misma se considera con las entregas de los ejercicios solicitados en cada trabajo práctico.
Aprobar el práctico final integrador con nota igual o superior a 7 (siete)
2. Por regularización: Obtener la regularización durante la cursada y aprobar un examen final Teórico/ Práctico en mesa de examen definida en calendario académico.
Para la obtención de la regularidad, el alumno debe:
1) Tener aprobados los Trabajos Prácticos solicitados, 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) la evaluación o alguna de sus dos recuperaciones, según lo establece la normativa vigente.
La materia no tiene la opción de aprobación en condición de LIBRE, dado las características de las actividades prácticas y la metodología de seguimiento y evaluación continua.

IX - Bibliografía Básica

[1] Enciclopedia de la Seguridad Informática. 2° ED. Alvaro Gomez Vieites. Ra-Ma. 2011
[2] Glosario de terminos de Ciberseguridad v2. Incibe. 2020.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
[3] Ley 25.326. Ley Argentina sobre Protección de Datos Personales.
https://www.argentina.gob.ar/sites/default/files/arg_ley25326.pdf
[4] Fundamentals of database systems. Ramez Elmasri, Shamkant B. Navathe. 7th ed. Pearson Education, 2017. ISBN: 978129209761
[5] Guía para Construir Aplicaciones y Servicios Web Seguros. 2005. OWASP.
https://owasp.org/www-pdf-archive/OWASP_Development_Guide_2.0.1_Spanish.pdf
[6] GUÍA DE PRUEBAS OWASP v3. 2008. OWASP. https://owasp.org/www-pdf-archive/OWASP_Testing_Guide_v3.pdf
[7] OWASP Top 10. OWASP. https://owasp.org/Top10/es/
[8] Web Security Testing Cookbook. O'Reilly. 2009. Paco Hope and Ben Walther
[9] Fundamentos De Seguridad En Redes. Aplicaciones Y Estándares. 2° edición. William Stallings. 2003

X - Bibliografia Complementaria

[1] Cloud Security and Privacy. Tim Mather, Subra Kumaraswamy, and Shahed Latif. 2009. O'Really
[2] Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados. Edición I. Raúl Siles Peláez. 2002. https://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/doc-seguridad-tcpip/Seguridad_en_TCP-IP_Ed1.pdf

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.

XII - Resumen del Programa

Unidad N°1. Introducción y conceptos básicos
Unidad N°2. Seguridad en el desarrollo de software
Unidad N°3. Seguridad en aplicaciones Web, Móviles y Base de datos
Unidad N°4. Seguridad en redes y Cloud

XIII - Imprevistos

XIV - Otros