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
SEGURIDAD DE LA INFORMACIÓN	LIC.CS.COMP.	RD-3-1/2023	2024	2° cuatrimestre

II - Equipo Docente

Docente	Función	Cargo	Dedicación
CASTRO, ALICIA DOMINGA MERCE	Prof. Responsable	P.Adj Exc	40 Hs
VALLEJO, ENRIQUE JORGE	Auxiliar de Práctico	A.1ra Semi	20 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 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 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.

En esta actividad curricular se abordan los siguientes ejes transversales:
• Identificación, formulación y resolución de problemas de informática.
• Gestión, planificación, ejecución y control de proyectos de informática.
• Utilización de técnicas y herramientas de aplicación en la informática.
• Fundamentos para el desempeño en equipos de trabajo
• Fundamentos para la comunicación efectiva
• Fundamentos para la acción ética y responsable
• Fundamentos para evaluar y actuar en relación con el impacto social de su actividad en el contexto global y local
• Fundamentos para el aprendizaje continuo
• Fundamentos para la acción emprendedora

VI - Contenidos

Contenidos mínimos: Conceptos básicos: Activos de información, incidentes, vulnerabilidades, riesgos, dimensiones de la seguridad de la información. Privacidad, Integridad y Seguridad de Sistemas de Información. Ciberataques: tipos, ciclo de vida. Mecanismos de protección: cifrado, control de acceso, autenticación y autorización, redundancia. Análisis de vulnerabilidades.
Los contenidos mínimos serán abordados en las siguientes unidades

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.

Actividad Práctica N.º 1: Introducción y conceptos básicos
Objetivos:
• Concientizar en los problemas asociados a ciberseguridad.
• Desarrollar la habilidad para identificar amenazas y vulnerabilidad de los activos de información.
• Analizar riesgos relacionados con la seguridad de la información.
• Identificar los activos críticos basados en los riesgos del negocio.
• Explicar los vectores de ataque y el ciclo de vida de un ataque.
La activad práctica incluye ejercicios donde se pretende que el estudiante:
• Reconozca las principales amenazas a la información y los actores de amenazas.
• Identifique y clasifique la información según la criticidad de la pérdida de confidencialidad, disponibilidad e integridad.
• Identifique los vectores de ataques y las vulnerabilidades existentes en un entorno informático.
• Desarrolle la capacidad de investigación en los problemas actuales de seguridad.
• Desarrolle la comunicación efectiva tras exposiciones orales y debates en grupos
• Comprensión de las técnicas, tácticas y procedimientos de un ciberataque, el cual puede utilizarse de un enfoque ético y responsable para el aseguramiento de la seguridad en un entorno informático.
• Analice el impacto y los riesgos de un ciberataque.

Actividad practica N.º 2. Seguridad en el desarrollo de software
Objetivos.
• Mostrar el ciclo de vida del desarrollo del software seguro
• Investigar sobre herramientas de testing en las diferentes etapas del desarrollo
• Identificar problemas de seguridad en el software.• Reconocer mecanismos de protección para el desarrollo del software.
• Informar sobre la legislación dirigida a la protección de la información personal, crediticia y de salud.
• Identificar los activos críticos y los riesgos asociados a los requerimientos legales
La actividad práctica incluye ejercicios donde se pretende que el estudiante:
• Reconozca los ítems asociados a la protección de la información en las legislaciones nacionales e internacionales, los activos de información asociados y los requerimientos de protección.
• Desarrolle acuerdos de confidencialidad en el proceso de desarrollo de software o de gestión en un entorno informático.
• Analice las acciones de protección de información en cada etapa del desarrollo del software
• Investigue sobre los software existentes para pruebas de seguridad en el desarrollo de software
• Desarrolle capacidad crítica para evaluar software identificando vulnerabilidades en el desarrollo.
• Reconozca mecanismos de seguridad para incorporar en las aplicaciones para crear un software seguro.

Actividad práctica N°3. Seguridad en aplicaciones Web, Móviles y Base de datos
Objetivos
• Identificar vectores de ataque en entornos web y aplicaciones móviles propuestos por OWASP

• Identificar amenazas y riesgos en entornos web.
• Realizar un análisis crítico sobre desarrollos inseguros
• Evaluar aplicaciones web vulnerables e identificar puntos a corregir.
• Identificar mecanismos de mitigación para el ciclo de desarrollo de aplicaciones móviles
• Aplicar protección a las bases de datos a nivel infraestructura y a nivel código de una aplicación.
La actividad práctica incluye ejercicios donde se pretende que el estudiante:
• Analice aplicaciones vulnerables e identifique posibles vectores de ataque
• Relacione los vectores de ataque con los riesgos asociados a la información
• Proponga mecanismos de mitigación en código vulnerable y en bases de datos
• Conozca herramientas de análisis de vulnerabilidades web y de base de datos.
• Investigue sobre las amenazas y riesgos en entornos web y el costo de pérdida de información.

Actividad práctica N°4. Seguridad en redes y Cloud
Objetivos
• Reconozca los vectores de ataque en infraestructuras de redes
• Identifique vulnerabilidades de servidores de aplicaciones y los riesgos a la información que pueden acarrear
• Analice las controles para mitigar los riesgos
La actividad práctica incluye ejercicios donde se pretende que el estudiante:
• Utilice herramientas que le permitan identificar vectores de ataque en una red.
• Conozca herramientas que le permitan visualizar las vulnerabilidades en una red
• Investigue sobre los ataques y mitigaciones en entornos cloud.

TRABAJO PRÁCTICO INTEGRADOR
Objetivo: Integrar los conceptos abordados durante la cursada de esta actividad curricular, a través de un caso de estudio dado.
En este Trabajo Práctico Integrador se realiza un proyecto. A partir de la unidad N.º 2 se entrega la consigna que involucra el contenido de distintas unidades. Se le solicita a los estudiantes entregas parciales correspondientes a subtareas del proyecto. Estas entregas tienen una corrección informada por parte del docente. Al finalizar la última entrega el alumno realiza una exposición comentando el trabajo realizado, con el objetivo que practique el desenvolvimiento oral y gane confianza para hablar frente a sus pares y docente.
Las actividades contemplan:
• Investigar sobre una herramienta dada y su aplicabilidad en un caso de estudio determinado.
• Desarrollar un informe escrito comentando las tareas realizadas, desde el análisis del caso de estudio, investigación de la herramientas, pasos de uso de la herramienta y resultados obtenidos, todo esto relacionándolo con los conceptos teóricos de la materia.
• Desarrollar una presentación con los puntos principales del trabajo, empleando lenguaje acorde a los contenidos de la materia.
• Exposición de la presentación

Estas actividades responden a los ejes temáticos:
Identificación, formulación y resolución de problemas de informática: En práctico 1 identificando amenazas, vulnerabilidades y ataques en un entorno informático.

Gestión, planificación, ejecución y control de proyectos de informática: En el practico N.º 1 y 2 y en la actividad práctica integradora donde se proponen casos de estudio donde el estudiante debe formular propuestas de proyectos para el desarrollo de aplicaciones seguras identificando los artífices del área de seguridad, cumplimiento y protección de datos.

Fundamentos para la comunicación efectiva y Fundamentos para el desempeño en equipos de trabajo: En los diferentes prácticos a través de las exposiciones orales y debates grupales.

Fundamentos para la acción ética y responsable: En el práctico 1 a través del análisis del accionar de un hacker ético. En el práctico 2 a través del desarrollo de acuerdos de confidencialidad y campañas de concientización para la sociedad y así disminuir los fraudes cibernéticos. En los prácticos 3 y 4 a través de la implementación de medidas de seguridad en el desarrollo del software para proteger a los usuarios de las aplicaciones como a la información procesada y almacenada por la misma.

Fundamentos para evaluar y actuar en relación con el impacto social de su actividad en el contexto global y local: Tras evaluar el impacto de los ciberataques en la sociedad y en el ámbito empresarial y la responsabilidad del profesional informático en el desarrollo de aplicaciones seguras, desarrollado en las distintas unidades.

Fundamentos para la acción emprendedora y Fundamentos para el aprendizaje continuo: En el práctico 1 tras investigar sobre los roles de personal de seguridad y conocimiento requerido por la industria generar un espíritu proactivo y de capacitación continua. En los diferentes prácticos se evalúan las soluciones de seguridad lo que deriva en evaluar las necesidades insatisfechas o ausentes que da posibilidad a idear y/o crear nuevas soluciones de seguridad.
Utilización de técnicas y herramientas de aplicación en la informática: Se aplica y se evaluá a través del uso de diferentes software para el desarrollo de las actividades prácticas solicitadas, a través de software de ofimática para el desarrollo de informes, presentaciones, etc, software asociado a Internet para búsqueda de información y uso de aplicaciones online colaborativas y herramientas especificas de seguridad de la información como son los analizadores de vulnerabilidades, cifrado, hash, entre otras.

La evaluación de los distintos ejes se realizará de forma continua utilizando distintas herramientas, desde cuestionarios, exposiciones informales y formales y con la presentación de ejercicios de los trabajos prácticos. Se pretende que el estudiante pueda medir su nivel de apropiación de los contenidos a medida que atraviesa cada unidad temática y al docente les brinda información acerca de la situación particular de cada estudiante para realizar un andamiaje adecuado en los casos que así lo requieran.

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