Facultad de Ingeniería - Universidad Nacional de Cuyo P2 - PLANIFICACIÓN DE CÁTEDRA			
Asignatura:	**Seguridad Informática**		
Profesor Titular:	**Mg. Bruno Roberti Ferri**		
Carrera:	**Licenciatura en Ciencias de la Computación**		
Año: 2023	**Semestre: 8no**	**Horas Semestre: 80**	**Horas Semana: 5**

1. PROGRAMA ANALÍTICO, PROGRAMA DE EXAMEN, BIBLIOGRAFÍA

Se informa en el Formulario P1 - Programa De Asignatura.

2. METODOLOGÍA DE ENSEÑANZA

La materia se organiza en clases que integran conceptos teóricos y prácticos, orientando el dictado a un modelo por competencias. Durante la clase se brindan los contenidos fundamentales de la asignatura y a continuación se desarrollan actividades de aprendizaje que propician la aplicación de los conceptos, modelos y metodologías que se van aprendiendo en el desarrollo de la asignatura y el uso adecuado de conceptos, y de terminología científico-tecnológica.

- Clases teórico-prácticas: Exposición de los temas teóricos correspondientes a cada unidad, apoyado con guías didácticas utilizando proyector multimedia. Luego se presentaban las herramientas o procedimientos a utilizar en la unidad, brindando al estudiante diversas fuentes de consulta para que pudiera avanzar en el cumplimiento de los objetivos planteados en los trabajos prácticos desarrollados. El desarrollo de los temas en clase debe ser completado con la lectura de la bibliografía recomendada, y con el material adicional que se presentará en clases
- Actividades Prácticas: Las actividades prácticas permiten ejercitar los temas cubiertos en la teoría, estas promuevan el desarrollo de habilidades para la resolución de problemas, la experimentación, el planteamiento de hipótesis, y el trabajo en equipo. La resolución de problemas debe conducir al desarrollo de las competencias necesarias para la identificación y solución de problemas de ingeniería, entendiendo como tal aquellas situaciones reales o hipotéticas cuya solución no es única y requiere la aplicación de los conocimientos de las ciencias básicas y de las tecnologías.
- Prácticas en laboratorio: Se utilizan los laboratorios informáticos disponibles en la Facultad configurados con las herramientas adecuadas para la resolución de las actividades prácticas pertenecientes a las unidades “Amenazas y Vulnerabilidades” y Análisis Forense. También se utiliza para la confección del Trabajo Práctico Integrador. Se implementan entornos de trabajo específicos mediante la utilización de máquinas virtuales orientadas a Seguridad Informática, fomentando la utilización de herramientas de código abierto. Se utilizan herramientas de Reconocimiento de redes, Escaneo de vulnerabilidades y Análisis de evidencia digital. También se utilizan sitios webs desarrollados para actividades prácticas compatibles con los objetivos de la asignatura.

- Trabajo Práctico Integrador: Presentación de un caso de estudio basado en los conceptos, procedimientos y herramientas desarrollados durante el cursado, el cual deberá abarcar la presentación de un Informe de Auditoría Técnica junto con toda la documentación de respaldo utilizada para la realización del mismo.

3. REGIMEN DE APROBACIÓN DE LA MATERIA

Consignado en programa de la asignatura.

4. EVALUACIONES PARCIALES

Las siguientes actividades realizadas por la plataforma se evaluarán. La evaluación para lograr la regularidad será formativa y sumativa.

Unidad a la que corresponde	Título del trabajo práctico/actividad de laboratorio/taller/etc.	Objetivo
1	Trabajo Practico 1: "Dimensiones de la Seguridad de la Información".	Investigación de la relación entre las dimensiones de la SI y los diferentes conceptos técnicos de la asignatura.
2	Actividad Lab. U2: "Configuración Herramientas PenTesting".	Instalar y configurar herramientas para realizar Test de Penetración en redes. Gestión de un entorno para pruebas.
2	Trabajo Practico 2: "Análisis de Vulnerabilidades"	Identificación y explotación de diferentes tipos de vulnerabilidades en un ambiente de prueba
3	Trabajo Practico 3: "Fortaleza de Contraseñas".	Aplicar procedimientos y herramientas para el análisis de la fortaleza de métodos criptográficas aplicados en contraseñas.
4	Trabajo Practico 4: "Desarrollo de un Dominio en la PSI".	Confección de un dominio de una política de Seguridad de la información basado en estándares internacionales.
5	Conferencia : "Metodologías de análisis de evidencia Forense Informática"	Investigar y exponer casos de aplicación sobre diferentes metodologías de análisis forense.
6	Actividad Virtual: "Metodología de Trabajo de la Auditoria Informática"	Identificar los objetivos de control a utilizar en una auditoría Informática y proponer procedimientos para su cumplimiento
1-2-3-4-6	TP Integrador: "Auditoría Gestión Informática" / "Auditoría Seguridad de la Información"	Ejecutar un proyecto de Auditoría de Seguridad Informática, que incluya toda la documentación de respaldo del mismo.

5. CONDICIONES PARA OBTENER LA PROMOCIÓN O REGULARIDAD

Consignado en programa de la asignatura.

6. INASISTENCIAS

Las inasistencias a clase deberán ser formalmente justificadas. Las inasistencias a los exámenes parciales y sus recuperatorios no serán justificadas.

7. REGIMEN ESPECIAL PARA ALUMNOS RECURSANTES

No hay régimen especial para alumnos recursantes

8. CRONOGRAMA

Detallar por mes y día el desarrollo del programa analítico, experiencias de laboratorio, salidas a campaña y evaluaciones parciales.

Semana N°	Unidad	Contenidos	Actividades	Cant. Hs.
1	1	Elementos y conceptos de la seguridad de la información. Dimensiones de SI. Activos de Información, Amenazas y Vulnerabilidades. Sistema de gestión de la seguridad de la información.		5
2	1	Introducción a la Criptografía. Esquemas simétricos y asimétricos. Función de dispersión criptográfica. Introducción a los Protocolos de Encriptación.	Desarrollo Trabajo Practico 1	5
3	2	Gestión de vulnerabilidades. Etiquetado e identificación. Evaluación de vulnerabilidades. Proyecto OWASP	Desarrollo Actividad U2	5
4	2	Software malicioso. Ingeniería social. Vulnerabilidades de bajo nivel y de red. Ataques a aplicaciones web.	Desarrollo Trabajo Practico 2	5
5	2	Introducción al Test de Penetración	Desarrollo Trabajo Practico 2	5
6	3	Técnicas de identificación y autenticación. Contraseñas, Certificados electrónicos y Biometria.	Desarrollo Trabajo Practico 3	5
7	3	Protocolos de Autenticación. Firma Electrónica. Modelos de Autorización. Control de Acceso Introducción a la Infraestructura de Clave Pública	Desarrollo Trabajo Practico 3	5
8	4	Política de Seguridad de la Información. Principales Dominios	Desarrollo Trabajo Practico 4	5
9	5	Introducción a la disciplina forense Informática Evidencia digital. Identificación y recolección. Manipulación	Desarrollo Trabajo Practico 4	5
10	5	Análisis de la evidencia digital e investigación Presentación e informe de resultados en distintos ámbitos.	Conferencias U5	5
11	6	Definición de Auditoria Informática. Tipos y áreas de aplicación. Proceso de Auditoría. Fases y Alcance. Metodologías de trabajo y Técnicas de Auditoría	Desarrollo TPI: Auditoria Seg. Inf.	5
12	6	Controles Auditoría Informática. Programa de Trabajo. Presentación e informe.	Desarrollo Actividad U6	5
13	1-6	Examen Parcial	Presentación Informe TPI	5
14	1-6	Coloquio Trabajo Práctico Integrador	Instancias de Recuperación.	5

Bruno Roberti

FECHA, FIRMA Y ACLARACIÓN TITULAR DE CÁTEDRA