Facultad de Ingeniería - Universidad Nacional de Cuyo P1- PROGRAMA DE ASIGNATURA			
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**

OBJETIVOS

- Identificar los descriptores sobre los cuales se asienta la seguridad de la información: confidencialidad, integridad, disponibilidad.
- Familiarizarse los algoritmos y protocolos criptográficos y su relación los aspectos de seguridad informática.
- Reconocer los conceptos de autenticación de la identidad, autorización y control de acceso.
- Definir y desplegar políticas de seguridad, orientadas tanto a la privacidad como a la confidencialidad, a la integridad, a la autenticación y a la disponibilidad..
- Conocer y comprender las vulnerabilidades y riesgos involucrados en los sistemas informáticos. Utilizar y configurar herramientas para el análisis de vulnerabilidades
- Aplicar técnicas de prevención, detección y mitigación de ataques.
- Aplicar una metodología forense informática, junto con el software específico, que abarque las etapas de recolección y análisis de evidencia digital.
- Aplicar procedimientos y técnicas de Auditoría de Seguridad Informática acorde las etapas de ejecución e informe de una auditoria.

DESCRIPTORES según Plan Estudios 2017:

Privacidad, integridad y seguridad en sistemas de información. Auditoría. Protocolos de encriptación y autenticación.

CONTENIDOS

UNIDAD 1: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

1.1. Elementos y conceptos de la seguridad de la información. Dimensiones
1.2. Activos de Información, Amenazas y Vulnerabilidades.
1.3. Sistema de gestión de la seguridad de la información. Componentes
1.4. Introducción a la Criptografía. Esquemas simétricos y asimétricos. Función de dispersión criptográfica.
1.5. Algoritmos de Cifrado DES y Diffie - Hellman.
1.6. Introducción a los Protocolos de Encriptación.

UNIDAD 2: AMENAZAS y VULNERABILIDADES

2.1. Gestión de vulnerabilidades.
2.2. Etiquetado e identificación. Evaluación de vulnerabilidades.
2.3. Proyecto OWASP
2.4. Software malicioso. Ingeniería social.
2.5. Vulnerabilidades de bajo nivel y de red.
2.6. Ataques a aplicaciones web.
2.7. Introducción al Test de Penetración

UNIDAD 3: IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROL DE ACCESO

3.1. Técnicas de identificación y autenticación.
3.2. Contraseñas, Certificados electrónicos y Biometria.
3.3. Protocolos de Autenticación. DSA y RSA. Firma Electrónica.
3.4. Modelos de Autorización. Control de Acceso
3.5. Introducción a la Infraestructura de Clave Pública

UNIDAD 4: POLITICA DE SEGURIDAD DE LA INFORMACIÓN

4.1. Estructura de una Política de Seguridad de la Información (Modelo ISO 27000).
4.2. Objetivos de Control. Categorías de Controles.
4.3. Aspectos Organizaciones SI.
4.4. Seguridad Física y del Entorno.
4.5. Autenticación, Autorización y Control de Accesos.
4.6. Seguridad de las Operaciones y Comunicaciones.

UNIDAD 5: ANÁLISIS FORENSE

5.1. Introducción a la disciplina forense Informática. Proceso Gestión de incidentes
5.2. Evidencia digital. Identificación. Metodología de Recolección y Manipulación.
5.3. Análisis de la evidencia digital e investigación. Análisis en Línea y fuera de Línea
5.4. Presentación e informe de resultados en distintos ámbitos.
5.5. Peritaje Informático

UNIDAD 6: AUDITORÍA DE SEGURIDAD INFORMÁTICA

6.1. Definición de Auditoria Informática. Tipos de Auditoría y áreas de aplicación. Equipo de Auditoría.
6.2. Proceso de Auditoría. Fases: Planeamiento – Ejecución – Informe – Seguimiento. Alcance de la Auditoría.
6.3. Metodologías de trabajo y Técnicas de Auditoría.
6.4. Controles Auditoría Informática: Definición, funciones y tipos de controles. Programa de Trabajo.
6.5. Elaboración y comunicación de Observaciones y Recomendaciones
6.6. El Informe de Auditoría.

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.

Actividad	**Carga horaria por semestre**
Teoría y resolución de ejercicios simples	30
Formación práctica	
Formación Experimental – Laboratorio	32
Formación Experimental – Trabajo de campo	
Resolución de problemas de ingeniería	18
Proyecto y diseño	
Total	**80**

Porcentaje de Horas Presenciales	100 % del Total
Porcentaje de Horas a Distancia	0% del Total

BIBLIOGRAFÍA

Bibliografía básica

Autor	Título	Editorial	Año	Ejemplares Biblioteca
Baca Urbina, Gabriel	Introducción a la Seguridad Informática. ISBN: 9786077444718 https://elibro.net/ereader/siduncu/40458	Editorial Patria	2016	eLibro.net
Gómez Fernández, Luis	Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad ISBN: 9788481439649 https://elibro.net/ereader/siduncu/53624	AENOR	2018	eLibro.net
Chicano Tejada, Ester	Auditoría de Seguridad Informática (MF0487_3). ISBN: 9788416433230 https://elibro.net/ereader/siduncu/44101	IC Editorial	2016	eLibro.net

Bibliografía complementaria

Autor	Título	Editorial	Año	Ejemplares Biblioteca
Alvaro Gómez Vieites	Auditoría de Seguridad Informática. ISBN 9788499643281 https://elibro.net/ereader/siduncu/62464	RA-MA	2014	eLibro.net
Gómez López, Julio	Hackers : aprende a atacar y a defenderte. ISBN: 9788499644608 https://elibro.net/ereader/siduncu/106449	RA-MA	2014	eLibro.net
Chicano Tejada, Ester	Gestión de incidentes de seguridad informática. (MF0488_3) ISBN: 9788416351701 https://elibro.net/ereader/siduncu/44136	IC Editorial	2014	eLibro.net
Stallings, W Brown, L	Computer Security: Principles and Practice 4th Edición. ISBN 9780134794105	Pearson/ Prentice Hall	2017	**0**
Keith J. Jones, R Bejtlich, C. Rose	Real Digital Forensics: Computer Security and Incident Response. ISBN: 9780321240699	Addison – Wesley	2005	**0**

EVALUACIONES

El régimen de evaluación se ajusta a lo establecido por la Ordenanza 108/10/CS- Anexo I, y a las normas reglamentarias específicas y resoluciones de casos particulares de la Facultad.

Evaluaciones durante el cursado

- Resolución de cuatro (4) trabajos prácticos, asociados a las unidades 1, 2, 3 y 4 de la asignatura. (TP)
- Resolución de dos (2) actividades, asociadas a las unidades 2 y 6 de la asignatura.
- Un examen parcial donde se evaluará aquellos conceptos teóricos-prácticos que sean relevantes para alcanzar la regularidad de la asignatura y que no se ven aplicados en el proyecto integrador o la conferencia grupal. (P)
- Conferencia grupal asociada a la metodología de análisis de evidencia Forense Informática. (C)
- Trabajo Práctico integrador el cual consiste en un proyecto de Auditoría de Seguridad Informática, asociado a un caso que se brindará para su resolución junto con la documentación de respaldo pertinente. El proyecto tiene 2 etapas, la primera es la presentación de un informe de auditoría junto con sus papeles de trabajo y la segunda un coloquio individual para demostrar el conocimiento teórico de los tópicos abarcados por el trabajo integrador. (TPI)

El ausente a las instancias de evaluación y la no presentación de los trabajos requeridos en el tiempo establecido será considerado como desaprobado.

Cada actividad y trabajo práctico, el examen parcial y la primer etapa el trabajo integrador tendrán su correspondiente instancia de recuperación en caso de obtener nota desaprobado en una entrega.

La conferencia y la etapa 2 del trabajo integrador no poseen instancia de recuperación, en caso de desaprobar no se puede acceder a la promoción directa.

Condición de regularidad tras el cursado

Regularizarán la materia aquellos estudiantes que hayan aprobado las actividades prácticas, el exámen parcial y el trabajo práctico integrador; o las instancias recuperatorias correspondientes con una nota igual o superior al 60%.

Condiciones de Promoción

Un estudiante promocionará la materia cuando:

- Aprueba cada una de las actividades prácticas o su instancia recuperatoria con una nota individual igual o superior a 60% respetando las fechas de entrega correspondientes.
- Aprueba con una nota igual o superior a 70% el examen parcial, el trabajo práctico integrador y la conferencia.
- Cumple con el 75% de asistencia a clases.

La nota final vendrá dada por la siguiente ecuación:

Nota final = TP1*0.10 + TP2*0.10 + TP3*0.10 + TP4*0.10 + C5*0.10 + P*0.20 + TPI*0.30

Evaluación final

El examen final es de tipo integrador teórico-práctico, de forma oral, y consiste en una evaluación teórica de los temas del programa y un coloquio basado en la carpeta del trabajo práctico integrador.

Debe presentarse la carpeta con el trabajo integrador aprobado con puntaje mayor o igual a 6 al momento del examen final. La evaluación teórica es a programa completo y actualizado.

Podrán rendir examen final los estudiantes que hayan obtenido la regularidad en la materia.

Alumnos recursantes.

No hay régimen especial para alumnos recursantes

Bruno Roberti

FECHA, FIRMA Y ACLARACIÓN TITULAR DE CÁTEDRA