Carrera INGENIERIA EN INFORMATICA		
Asignatura 3666 - Seguridad Aplicada y Forensia		
Trayecto Calidad y Seguridad de la Información		
Año académico 2023		
Responsable / Jefe de catedra Mg. Ing. Cintia Gioia		
Carga horaria semanal 4 hs.	**Carga horaria total** 64 hs.	**Créditos** -----
Modalidad Presencial		
Correlativas anteriores AUDITORIA Y LEGISLACION – PROGRAMACION AVANZADA - SISTEMAS OPERATIVOS	**Correlativas posteriores** ELECTIVA II	
Conocimientos necesarios Seguridad de la Información - Ciberseguridad - Redes informáticas – Sistemas Operativos – Auditoría de Seguridad de la Información – Nociones de Criptografía – Legislación vigente aplicable al ejercicio profesional del Ingeniero en Informática - Delitos Informáticos – Protección de Datos Personales.		

Descripción de la asignatura

La asignatura proporciona sólidos conocimientos teóricos-prácticos relacionados a la aplicación de la informática forense y los conceptos fundamentales de la seguridad aplicada al ciclo del desarrollo del software y el hacking ético.
Con el aumento y perfeccionamiento de las conductas delictivas que llegan a la justicia y que involucran dispositivos informáticos surge la necesidad de acudir cada vez más a expertos en informática forense, siendo crucial su actuación en materia probatoria. La materia se enfoca en que el alumno aprenda los elementos y aspectos teórico prácticos fundamentales de la informática forense con la finalidad que adquiera las habilidades necesarias para resolver problemas concretos, del sector público y privado, donde se requieran aplicar procedimientos y metodologías para el tratamiento de la evidencia digital y la puesta en práctica de técnicas y herramientas forenses en distintos escenarios y tecnologías, considerando el marco legal y procesal vigente.
Se capacita a los alumnos sobre técnicas de intrusión, modalidad de ataques y defensa, la seguridad en el ciclo de desarrollo de software, logrando que se involucren con la filosofía y el accionar del mundo del Hacking Ético, conociendo las herramientas y metodologías necesarias para realizar tareas de análisis de vulnerabilidades, test de penetración y evaluaciones de seguridad, aplicados siempre bajo la ética profesional. Asimismo, se interioriza al alumno en las técnicas de seguridad defensiva y ofensiva para optimizar la protección ante ataques informáticos, como también la respuesta a incidentes.

Metodología de enseñanza

La metodología de enseñanza se focaliza en clases teóricas con la ejemplificación de la aplicación de los mismos en escenarios, de manera de lograr que el alumno obtenga un conocimiento equilibrado de los componentes teóricos y aplicación de los mismos en escenarios reales. La materia desarrolla una capacitación integral que incluye desde el aprendizaje de conceptos fundamentales, como también entrenamientos prácticos basados en casos simulados sobre escenarios ficticios adaptados de la realidad y planteados para la aplicación de las diversas técnicas y uso de herramientas. Se basa en la utilización de técnicas

y de las tecnologías más relevantes del mercado y en una permanente innovación y actualización académica.

Los contenidos de la asignatura se presentan de forma iterativa e incremental. Se asume la enseñanza basada en problemas, ya que esto favorece la construcción del aprendizaje mediante la investigación, interpretación, argumentación y propuesta de una posible solución. De esta forma, los estudiantes desarrollan sus capacidades, participando en escenarios simulados relevantes, que facilitan la conexión entre la teoría y su aplicación. Logrando convertir la información en conocimiento y desarrollar el pensamiento, más allá de la memorización.

Las clases serán dictadas a través de distintos métodos, como explicaciones a través de definiciones, ejemplos, ejercicios, lectura individual dirigida, actividades grupales de análisis, transferencia, validación colectiva y exámenes. Determinados contenidos temáticos serán presentados a los alumnos a través de proyecciones y videos. Las diversas actividades teórico-prácticas planteadas favorecen la investigación, el desarrollo, el trabajo en equipo y la fijación de conocimientos.

Se llevan a cabo diferentes trabajos prácticos orientados a desarrollar alguna actividad práctica ya sea aplicando alguna metodología, procedimientos o utilizando herramientas específicas. Se desarrollarán diferentes prácticos individuales y/o grupales aplicando los contenidos dados en las diferentes unidades temáticas, para poder fijar los conocimientos de forma práctica. Se fomentará al alumno al trabajo en grupo. Se realizará un seguimiento de los estudiantes por cada uno de los trabajos que se planteen.

El proceso de enseñanza y de aprendizaje de carácter teórico-práctico, permanente e integral, propone a los alumnos la adquisición de conocimientos, el desarrollo de actitudes y la detección de aptitudes, el aumento de la destreza y las habilidades para comprender y encontrar información relevante, y la resolución de las situaciones nuevas que se le presenten, utilizando un enfoque hacia la resolución de problemas.

El alumno debe mostrar al finalizar el curso un nivel mínimo de destreza en los conceptos y las tecnologías específicas asociadas a la materia.

Considerando que la adaptación a las nuevas tecnologías supone un reto fundamental actual, se le facilitará al alumno la posibilidad y los medios necesarios para que puedan acceder, conocer e investigar todos los instrumentos que las nuevas y últimas tecnologías ofrecen.

Se motiva a los estudiantes el uso de la plataforma MIEL para acceder al material, usar el foro, para comunicaciones con la cátedra y para la resolución de dudas tanto de conceptos teóricos como prácticos. Se utilizará la plataforma de MS Teams para las clases que se dicten de manera virtual sincrónica. La cátedra cuenta con soporte audiovisual de parte de los contenidos, que los alumnos pueden consultar luego de haber asistido a la clase.

Metodología de Clases Teóricas

- Las clases teóricas están orientadas a introducir a los alumnos en los diferentes conceptos teóricos conceptuales de la materia.

- Cada tema teórico es abordado en clase brindando el profesor ejemplos de aplicación.
- La metodología de trabajo alternará entre clases expositivas donde los profesores explicarán los temas y otras haciendo participar a los alumnos mediante exposición dialogada.

Metodología de Clases Prácticas

- Las clases prácticas se referirán a cada núcleo temático de la materia o podrán integrar conceptos de diferentes unidades.

Trabajos Prácticos

- Para poder realizar un seguimiento progresivo del aprendizaje, se asocian a determinadas unidades temáticas trabajos prácticos en la que los alumnos podrán aplicar lo aprendido.
- Se desarrollarán trabajos prácticos donde se hará hincapié en algún concepto fundamental o combinación de los mismos, para luego comprender los resultados en base a los procedimientos aplicados.
- Estos trabajos prácticos posibilitan la resolución de problemas por unidad temática o integrando varias unidades, con objetivos específicos. Consisten en planteos de problemas y actividades referentes a los diversos contenidos de la asignatura.
- Los trabajos prácticos serán seleccionados con un criterio que pondere lo conceptual y lo estratégico en lugar de la mecanización de procedimientos.
- Los trabajos prácticos pueden variar en cada cuatrimestre, considerando además los avances tecnológicos y de contenido de la materia.
- Se plantearán trabajos prácticos obligatorios y complementarios. Los docentes corregirán cada trabajo práctico entregado por los alumnos y darán una devolución personalizada.
- Esto trabajos estarán destinados a aplicar y medir el grado de comprensión de los temas teóricos expuestos en clase y el manejo de las definiciones y propiedades en contextos prácticos para comprobar que realmente se han incorporado los conceptos y no memorizado o mecanizado definiciones, procedimientos y demostraciones presentadas en las clases .
- Los trabajos tienen como finalidad generar la capacidad necesaria para saber interpretar claramente los objetivos del problema y poder resolverlo, aplicando una adecuada estrategia en la resolución.
- El docente irá evaluando el progreso de cada alumno en cada entrega de los diferentes prácticos (sean grupales o individuales).
- Los alumnos deberán ir realizando entregas parciales de avances establecidas por el docente durante la cursada.

Plataforma y Materiales Didácticos

- La materia cuenta con apuntes teórico-prácticos desarrollados por los profesores de la cátedra. También se utilizan los libros detallados en la sección de Bibliografía.
- Se motiva a los estudiantes el uso de la plataforma MIEL para acceder al material, usar el foro, para comunicaciones con la cátedra y para la resolución de dudas tanto de conceptos teóricos como prácticos.

Objetivos de aprendizaje

- Comprender el crecimiento de conductas indebidas o ilegales donde los dispositivos informáticos y la información son el medio o incluso el fin u objeto del delito.
- Comprender los principios fundamentales de la informática forense.
- Estudiar los diferentes procedimientos y metodologías en todo el ciclo de tratamiento de la evidencia digital.
- Conocer los protocolos, normas y guías de buenas prácticas, así como los fundamentos legales y procesales de la informática forense.
- Adquirir los conocimientos y habilidades técnicas sobre las últimas metodologías, técnicas, tecnologías y herramientas a aplicar en escenarios de tratamiento de evidencia digita
- Conocer los fundamentos y los desafíos de la investigación forense de dispositivos móviles.
- Conocer los principales mecanismos que utilizan los ciberdelincuentes para ocultar, encriptar y encapsular información.
- Identificar incidentes de seguridad informática que requieran la aplicación de análisis forense digital.
- Tomar conciencia respecto a la importancia de incorporar la seguridad en el proceso de desarrollo de software adquiriendo una visión general del escenario de seguridad actual y los vectores de amenazas emergentes.
- Conocer los lineamientos generales necesarios para fortalecer el ciclo de desarrollo de software desde la perspectiva de la seguridad y manejar en detalle las principales prácticas que defina la industria.
- Comprender las técnicas de intrusión, modalidad de ataques y defensa.
- Conocer las metodologías y herramientas necesarias para realizar tareas de análisis de vulnerabilidades y tests de penetración, con una filosofía enfocada a la ética profesional.
- Conocer los fundamentos de la Seguridad Defensiva y ofensiva.
- Comprender como llevar a cabo un análisis de software malicioso.
- Reconocer la importancia de la gestión de incidentes en las organizaciones.

Contenidos mínimos

Seguridad en el Ciclo de Vida de Desarrollo de Software. Introducción al Hacking Ético. Pruebas de intrusión. Análisis de Vulnerabilidades. Estándares y metodologías de prueba y verificación de seguridad de aplicaciones. Fundamentos de Informática Forense. Tratamiento de la Evidencia Digital. Aspectos procesales en la actuación pericial.

Competencias a desarrollar

Genéricas

- Identificación, formulación y resolución de problemas de ingeniería en sistemas de información/informática.
- Utilización de técnicas y herramientas de aplicación en la ingeniería en sistemas de información / informática.
- Actuación profesional ética y responsable.

- Aprendizaje continuo.
- Concepción, diseño y desarrollo de proyectos de ingeniería en sistemas de información / informática.
- Gestión, planificación, ejecución y control de proyectos de ingeniería en sistemas de información / informática.
- Desempeño en equipos de trabajo.
- Comunicación efectiva.
- Evaluación y actuación en relación con el impacto social de su actividad profesional en el contexto global y local.

Específicas

- Proyecto y dirección en lo referido a seguridad informática.
- Procedimientos y certificaciones del funcionamiento, condición de uso o estado de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software.
- Dirección y control de la implementación, operación y mantenimiento de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software.
- Especificación, proyecto y desarrollo de software.
- Establecimiento de métricas y normas de calidad de software.
- Especificación, proyecto y desarrollo de sistemas de información.
- Especificación, proyecto y desarrollo de sistemas de comunicación de datos.

Programa Analítico	
Unidad 1	**Fundamentos de la ciencia forense digital** Fundamentos de la ciencia forense digital. Definición y fases de la Informática Forense. Evidencia digital. Metodologías de tratamiento de evidencia digital. Correlación entre distintas clases de evidencia digital. Protocolos, normas y guías de buenas prácticas. Marco Legal. Aspectos procesales fundamentales. Modalidades delictivas informáticas.
Unidad 2	**Procedimientos para la investigación científica en escenas del hecho** Procedimientos en escenas del hecho. Protocolos vigentes de Ministerios Públicos, fuerzas policiales y de seguridad**.** Cadena de custodia. Escenarios de adquisición de evidencia digital. Recolección de evidencia digital en sistemas vivos y muertos. Captura de memoria RAM.
Unidad 3	**Secuestro de evidencia digital y cadena de custodia** Cadena de custodia. Reglamentos vigentes. Tipos de documentación en procesos judiciales. Formulario de cadena de custodia. Protocolos para levantamiento y conservación de la evidencia. Preservación de la evidencia digital. Aislamiento. Jaula de Faraday. Secuestro, clasificación, embalaje y transporte de objetos.
Unidad 4	**Plataformas, herramientas y tecnologías forenses**

	Plataformas, herramientas y tecnologías forenses aplicables a las distintas fases de tratamiento de la evidencia digital y según la naturaleza de esta. Software licenciado vs. software no licenciado. Tipos de licencias, alcances y limitaciones. Primera aproximación a un software forense. Prácticas de técnicas periciales básicas.
Unidad 5	**Verificación de la integridad de los datos** Integridad de los datos. Funcionamiento y aplicación de los algoritmos hash. Funciones. Calculo Hash. Ejemplo de casos. Bases de datos. Aplicación y verificación de la integridad de los datos.
Unidad 6	**Adquisición y procesamiento de imágenes forenses** Bloqueadores de escritura por hardware o software. Adquisición de evidencias. Adquisición de imagen forense. Formatos de adquisición de imágenes forenses. Adquisición y montaje. Aplicación de software forenses para generar y gestionar las imágenes forenses. Almacenamiento de la evidencia digital.
Unidad 7	**Análisis forense** Análisis Forense. Principales razones que desencadenan un análisis forense. Introducción al proceso de investigación del cibercrimen. Denuncia e intervención del laboratorio de informática forense. Diferentes tipos de laboratorios de informática forense. Desintervención. Evidencia digital y cadena de custodia. Pericias informáticas. Puntos de pericia. Métodos y procedimientos técnicos del análisis forense.
Unidad 8	**Procesamiento de imágenes forenses e investigación de metadatos** Procesamiento de imágenes forenses. Búsqueda de información específica. Visualización de línea de tiempo, historial y registro de eventos. Metadatos y su tratamiento. Extracción y modificación de metadatos. Análisis forense de imágenes.
Unidad 9	**Recuperación de archivos eliminados** Conceptos relacionados al borrado de archivos. Recuperación de archivos eliminados. Herramientas y técnicas de recuperación de archivos eliminados mediante “recovery” y “carving”. Borrado seguro. Desintegración.
Unidad 10	**Presentación de resultados de análisis forenses** Consideraciones básicas. Informe técnico e informe gerencial. Estructura general del informe. Redacción del informe. Ejemplos de presentación de resultados. Asistencia a juicio y oratoria.
Unidad 11	**Técnicas Antiforense** Conceptos de Anti-Forensia. Técnicas y herramientas antiforenses. Ofuscación, ocultamiento, eliminación y la no generación de datos. Cifrado de información. Fundamentos del anonimato. Investigación de IP. Anonimato a través de VPN (red privada virtual) y redes de anonimato

	(como redes Tor). Gestor de contraseñas. Análisis de correos electrónicos. Correos electrónicos comprometidos.
Unidad 12	**Análisis forense aplicado a dispositivos móviles y tecnologías especiales** Introducción a dispositivos de telefonía móviles. Evolución. Hardware. Software. Sistemas Operativos. Arquitectura de los sistemas. Modelos de seguridad. Fundamentos del análisis forense en dispositivos móviles. Plataformas, herramientas y tecnologías forenses aplicables a extracción y análisis de evidencia digital en dispositivos móviles. Desafíos en las técnicas de investigación forense en dispositivos móviles. Extracción de datos e información. Análisis forense de datos extraídos. Introducción a técnicas avanzadas como alternativas para el análisis forense de dispositivos móviles. Introducción al análisis forense sobre tecnologías especiales o nuevas.
Unidad 13	**Introducción a la seguridad en el ciclo de vida del desarrollo del software** Seguridad en el ciclo de vida de desarrollo de Software. Seguridad en el análisis, diseño, desarrollo, testing e implementación. Integración de la seguridad durante todo el ciclo de vida de las tecnología de información (DevSecOps: Desarrollo, Seguridad y Operaciones). Controles preventivos, detectivos y correctivos. Controles automatizados de seguridad en el ciclo de vida de desarrollo de Software. Vulnerabilidades de seguridad en el software. Reconocimiento y detección proactiva de las falencias del desarrollo de las aplicaciones. Guías de desarrollo seguro. Técnicas de desarrollo seguro. Proyecto abierto de seguridad de aplicaciones (OWASP).
Unidad 14	**Introducción al Hacking Ético** Fundamentos del Hacking Ético. Alcances e implicancias. Códigos de ética. Tipos y técnicas de ataques (a sistema operativos, aplicaciones, infraestructuras y diversas tecnologías). Fases de un ataque. Evaluaciones de seguridad. Evaluaciones de vulnerabilidades. Test de intrusiones. Metodologías y etapas. Reconocimientos activos y pasivos. Análisis de brecha de cumplimiento. Informes. Seguridad Defensiva (Blue Team) y Seguridad Ofensiva (Red Team): funciones y diferencias. Ciberinteligencia. Ataques por Ingeniería social.
Unidad 15	**Análisis de software malicioso** Software Malicioso (Malware). Características y estructuras de los Malware. Clasificación de los Malware. Acciones de los atacantes. Análisis del Malware. Tipos de análisis del Malware. Ocultamiento y eliminación de archivos. Minimización de huellas. Aplicaciones de seguridad.
Unidad 16	**Gestión de Incidentes** Equipos de Respuesta a Incidentes de Seguridad (CSIRT, CERT). Misión y funciones. Gestión de incidentes. Tipos de incidentes. Técnicas de respuesta ante incidentes. Gestión y revisión de logs. Monitoreo de eventos. Normativas vinculadas.

Planificación de actividades					
Semana	**Clase**	**Actividad** [Detalle de la actividad a desarrollar]	**Tipo** [indicar el tipo de actividad a desarrollar: teoría, practica, practica de laboratorio, trabajo de campo, otra]	**Duración estimada**	**Unidad/des**
Semana 1	Fundamentos de la ciencia forense digital	Presentación	Teoría	4 horas	Unidad 1
Semana 2	Procedimientos en escenas del hecho	Presentación	Teoría	4 horas	Unidad 2
Semana 3	Secuestro de evidencia digital y cadena de custodia	Taller	Práctica	4 horas	Unidad 3
Semana 4	Plataformas, herramientas y tecnologías forenses	Presentación y Taller	Teoría y Práctica de laboratorio	4 horas	Unidad 4
Semana 5	Verificación de la integridad de los datos. Adquisición y procesamiento de imágenes forenses.	Presentación y Taller	Teoría y Práctica de laboratorio	4 horas	Unidad 5 Unidad 6
Semana 6	Análisis Forense	Presentación	Teoría y Práctica de laboratorio	4 horas	Unidad 7
Semana 7	Procesamiento de imágenes forenses e investigación de metadatos	Presentación y Taller	Teoría y Práctica de laboratorio	4 horas	Unidad 8

Semana 8	PARCIAL Recuperación de archivos eliminados	PARCIAL Presentación y Taller	Evaluación teórica y práctica Teoría/Práctica	2 horas 2 horas	Unidad 1 a 8. Unidad 9
Semana 9	Presentación de resultados, mediante reporte e informes técnicos. Técnicas Anti-Forense	Presentación	Teoría/Práctica	4 horas	Unidad 10 Unidad 11
Semana 10	Técnicas Anti-Forense	Taller	Práctica	4 horas	Unidad 11
Semana 11	Introducción a análisis forense de dispositivos móviles y tecnologías especiales	Presentación. Demostraciones.	Teoría. Práctica.	4 horas	Unidad 12
Semana 12	Introducción a la seguridad en el ciclo de vida del desarrollo del software	Presentación	Teoría	4 horas	Unidad 13
Semana 13	Introducción al Hacking Ético. Análisis de Software Malicioso.	Presentación. Demostraciones.	Teoría	4 horas	Unidad 14 Unidad 15
Semana 14	Análisis de Software Malicioso. Gestión de Incidentes.	Presentación. Demostraciones.	Teoría. Práctica.	4 horas	Unidad 15 Unidad 16

Semana 15	PARCIAL Devolución de Práctico Grupal	PARCIAL Exposición, defensa y devolución de trabajo práctico.	Evaluación	4 horas	Unidad 9 a 16
Semana 16	RECUPERATORIO Devolución de Trabajo Práctico (que requieran recuperatorio)	RECUPERATORIO Exposición, defensa y devolución de trabajo práctico.	Evaluación	4 horas	

Evaluación
El proceso evaluativo se basa en dos exámenes parciales presenciales y un examen recuperatorio presencial (en el cual se puede recuperar uno de los dos parciales). Las evaluaciones serán escritas y prácticas, pudiendo la cátedra llevar a cabo evaluaciones orales y/o en la PC. En el primer parcial se evaluarán las unidades 1 a la 8, por medio de preguntas teóricas y prácticas. El segundo parcial se evaluarán las unidades 9 a 16 utilizando una metodología similar, pero se agregan más ejercicios prácticos. Además los alumnos deberán desarrollar los trabajos prácticos obligatorio durante el cuatrimestre, los cuales tendrá un seguimiento periódico quincenal. En el caso que el alumno cumpla con los requisitos establecidos en el Régimen de Cursada pero no con los criterios de promoción, deberá rendir un examen final, los cuales se confeccionarán de manera de poder evaluar la parte teórica/práctica integral de la materia. Para poder rendir el examen libre, el alumno deberá contactar al inicio del primer cuatrimestre o del segundo cuatrimestre a los docentes de la materia, a fin de solicitar el acceso al material actualizado y además el enunciado de los trabajos prácticos especiales que deberá entregar y aprobar, previo a rendir el final. Si el alumno no entregara y aprobara, previo al examen final libre, los trabajos prácticos especiales, no estará en condiciones de rendir el examen final libre.

Primera evaluación	Semana 8	Evaluación Teórica/Práctica	2hs.
Segunda evaluación	Semana 15	Evaluación Teórica/Práctica	2 hs.
Recuperatorio	Semana 16	Evaluación Teórica/Práctica	2 hs.

Bibliografía obligatoria				
Titulo	**Autor**	**Editorial**	**Edición**	**Año**

Computación forense, descubriendo los rastros digitales	Jeimy José Cano Martínez	Alfaomega Grupo Editor	Físico	2016
Técnicas de análisis forense informática para peritos judiciales profesionales.	Pilar Vila Avendaño	ZeroXwoed Computing,	Físico	2018
El rastro digital del delito, aspectos técnicos, legales y estratégicos de la informática forense	Universidad FASTA	Universidad FASTA	Digital	2017

Bibliografía complementaria recomendada				
Titulo	**Autor**	**Editorial**	**Edición**	**Año**
Guidelines for digital forensics first responders	INTERPOL	INTERPOL	Digital	2021
Guía integral de empleo de la informática forense en el proceso penal	Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense	InFoLab	Digital	2016
Convenio sobre la ciberdelincuencia	Consejo de Europa	Consejo de Europa	Digital	2001
Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia	Consejo de Europa	Consejo de Europa	Digital	2022

Otros recursos obligatorios [Videos, enlaces, otros. Incluir una fila por cada recurso]	
Nombre	

Otros recursos complementarios [Videos, enlaces, otros. Incluir una fila por cada recurso]	
Nombre	