CÓDIGO DE ASIGNATURA
1112

ASIGNATURA: Auditoría y Seguridad Informática

REFERENTE DE CÁTEDRA: Mg. Ing. Cintia Verónica Gioia

AÑO: 2020

CARGA HORARIA: 4

OBJETIVOS:

Los **propósitos fundamentales** de esta asignatura son:

Objetivos Generales:

- Familiarizar al alumno en los conceptos y términos básicos y avanzados del área de auditoria y seguridad informática.
- Que el alumno adquiera los conocimientos necesarios para garantizar y auditar la integridad, disponibilidad, privacidad, control y autenticidad de la información digital.
- Capacitar al alumno en medidas de protección de seguridad físicas, lógicas y procedimentales contra eventos que pudieran llevar a la adquisición y transferencia indebida de datos, modificación o distribución ilegítima de los mismos o bloqueo de los sistemas.
- Identificar, proponer y resolver situaciones o eventos vinculados a la seguridad de la información.

Objetivos Específicos:

- Conocer las estrategias para la identificación de los activos de información y la implementación de políticas, estándares, procedimientos y guías de acuerdo con su nivel de riesgo.
- Interiorizar a los alumnos en principios, tecnologías, metodologías y estándares empleados para asegurar y controlar la disponibilidad, integridad y confidencialidad de sistemas, equipos, redes y la información contenida o transmitidas a través de los mismos.
- Conocer las técnicas y mecanismos de protección de instalaciones físicas.

- Aplicar e implementar principios de administración de red segura, distinguir y diferenciar elementos y componentes de una red, así como implementar y utilizar protocolos comunes.
- Identificar los elementos para asegurar la seguridad en el Ciclo de Vida de Desarrollo de Software.
- Conocer las metodologías y herramientas para asegurar la continuidad del negocio de las organizaciones en el caso de producirse situaciones críticas que pudieran detener la operación normal de la misma.
- Introducir al alumno en aspectos legales relacionados con los contratos informáticos, licenciamiento del software, propiedad intelectual y la protección de datos personales.
- Familiarizarse con las leyes y regulaciones de los delitos informáticos, las técnicas y medidas de investigación, análisis de evidencia digital y códigos de ética.
- Introducir al alumno los conceptos generales relacionados con la criptografía y su aplicación.

CONTENIDOS MÍNIMOS:

Introducción a la Seguridad Informática. Seguridad Física. Seguridad Lógica. Seguridad en Redes. Norma IRAM-ISO/IEC 27001. Norma IRAM-ISO/IEC 27002. Gestión de Riesgos Business Continuity & Disaster Recovery Plan. Contratos Informáticos. Licencias. Derecho de Autor y Propiedades. Auditoria de Sistemas. Estándar COBIT. BCRA 4609. Protección de Datos Personales. Peritaje Forense Informática. Delitos Informáticos. Modalidades de delitos informáticos. Ciberseguridad. Ransomware. Ingeniería Social y Ataques Informáticos. Informática Forense e Investigación Digital. Seguridad en el Ciclo de Vida del Desarrollo (SDLC). Introducción a OWASP. Penetration testing execution standard (PTEST). Application Security Verification Standard. VEGA. Introducción a la Criptografía. Criptomonedas

Correlatividades: 1026 - Tecnología, Ingeniería y Sociedad
1109 - Arquitectura de Computadoras

PROGRAMA ANALÍTICO:

Unidad n° 1: Seguridad Informática

- Introducción a la Seguridad Informática.
- Conceptos de confidencialidad, integridad y disponibilidad.
- Amenazas. Vulnerabilidades.
- Políticas de seguridad informática.
- Seguridad lógica. Autenticación. Métodos de control de acceso.
- Seguridad física. Controles de Seguridad Física.

- Ciberseguridad. Infraestructuras críticas.
- Ransomware.
- Ingeniería Social y Ataques Informáticos.

Unidad n° 2: Estándares

- Introducción a los estándares internacionales de Seguridad de la Información.
- Normas BS. Normas Common Criteria. Estándares del NIST.
- Normas ISO, serie 27000.
- Norma IRAM-ISO/IEC 27001.
- Norma IRAM-ISO/IEC 27002.
- Norma ISO 27005. Gestión de Riesgos.
- BCP/DRP. Business Continuity & Disaster Recovery Plan.

Unidad n° 3: Auditoria Informática

- Introducción a la auditoría y consultoría.
- Control interno informático y auditoria informática.
- Plan auditor. Introducción a la metodología COBIT.
- Criterios de Información. Recursos de TI. Dominios de control.
- Marco COBIT.
- Auditoría interna de los Sistemas de gestión.
- Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras (BCRA 4609).

Unidad n° 4: Peritajes

- Introducción a las pericias informáticas.
- Perfil del perito informático.
- Pasos de una pericia.
- El informe pericial.
- Leyes vinculadas a la actividad del perito informático.
- El análisis forense informático.
- Herramientas de hardware y software.
- Informática Forense e Investigación Digital.

Unidad n° 5: Características de seguridad en la transmisión de datos

- Introducción a la seguridad en redes.
- Vulnerabilidades de las Redes.
- Diseño seguro de redes. Firewalls: distintos tipos.
- IDS: Intrusion Detection Systems.
- IPS: Intrusion Prevention Systems.
- V-LAN’s: redes virtuales.
- Análisis de LOGs.

Unidad n° 6: Licencias de Software

- Introducción a al licenciamiento del software.
- Distintos tipos de licenciamiento del software.
- Introducción al concepto de SaaS – Software as a Service.
- Aplicaciones en Cloud Computing.
- Licencias de software libre.

Unidad n° 7: Contratos Informáticos

- Introducción a los contratos informáticos.
- Aspectos a considerar en los contratos informáticos.
- Acuerdo de nivel de servicios – SLA.
- Cumplimiento y sanciones.
- Norma ISO 20000-1, Calidad de Servicios de TI.

Unidad n° 8: Patentes

- Introducción al concepto de Propiedad Intelectual.
- Protección del software y de las bases de datos.
- Ley de Propiedad Intelectual.

Unidad n° 9: Aspectos legales

- Introducción al derecho informático.
- Seguridad y privacidad de los datos.
- El marco normativo de las nuevas tecnologías.
- Ley de firma digital.
- Ley de protección de los datos personales.
- Ley de delitos informáticos.
- Modalidades de delitos informáticos.

Unidad n° 10: Seguridad en el Desarrollo de Software

- Seguridad en el Ciclo de Vida de Desarrollo de Software (SDLC).
- Introducción a OWASP (Open Web Application Security Project).
- Estándar de verificación de seguridad de aplicaciones (ASVS, Application Security Verification Standard).
- Estándar de Ejecución de Pruebas de Penetración (PTES).
- Estándar de Ejecución de Pruebas de Penetración (PTES).

BIBLIOGRAFÍA:

BIBLIOGRAFÍA BÁSICA

(Debe existir en Biblioteca o estar disponible para la compra)

Autor	Título	Editorial	Año	Edición

BIBLIOGRAFÍA COMPLEMENTARIA

Autor	Título	Editorial	Año	Edición
Hugo D. Scolnik	Qué es la seguridad informática	PAIDOS	2012	1era
Ana Haydeé Di Iorio y otros	El Rastro Digital del Delito	Universidad FASTA Ediciones	2017	1era
Daniel Dupuy, Mariana Kiefer	Cibercrimen	BdeF	2016	1era
Daniel Dupuy, Mariana Kiefer	Cibercrimen II	BdeF	2018	1era
Jeimy Cano	Computación Forense. Descubriendo los Rastros Informáticos	Alfaomega	2016	1era

METODOLOGÍA DE ENSEÑANZA:

Metodología General de Clases

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.

A modo complementario se llevan a cabo diferentes trabajos prácticos orientados a desarrollar alguna actividad práctica ya sea aplicando alguna metodología o estándar o utilizando herramientas específicas.

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.

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.

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.

Las diversas actividades teórico-prácticas planteadas favorecen la investigación, el desarrollo, el trabajo en equipo y la fijación de conocimientos.

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.

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 integrarán conceptos.

Trabajos Prácticos Por Unidad Temática

- 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.
- 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.

- Estos trabajos prácticos posibilitan la resolución de problemas por unidad temática con objetivos propios, y consisten en planteos de problemas y actividades referentes a los diversos contenidos de la asignatura.
- El docente irá evaluando el progreso de cada alumno en cada entrega de los diferentes prácticos grupales o individuales.
- La presentación de los trabajos prácticos será guiada por los objetivos propuestos para el tema específico al cual la práctica se refiere.
- 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.

Trabajos Prácticos Integradores

- Para poder realizar un aprendizaje integral de la aplicación de todos los contenidos de la materia se podrán planteará trabajos prácticos integradores a los cuales se irán agregando poco a poco cada uno de los conceptos aprendidos durante la cursada.
- 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 e integradores para comprobar que realmente se han incorporado los conceptos y no memorizado o mecanizado definiciones, procedimientos y demostraciones presentadas en las clases o que figuran en los libros.
- Los trabajos integradores 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 alumno deberá ir realizando entregas parciales de avances establecidas por el docente durante la cursada. El docente hará seguimiento del alumno en cada entrega y exposición del práctico.

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.

Sitio Web: MIEL

- Sitio web destinado a facilitar al alumno el acceso al programa de la materia, material de estudio, ejemplos, trabajos prácticos, entre otros archivos y el contacto directo con docentes y alumnos.

EXPERIENCIAS DE LABORATORIO/ TALLER / TRABAJOS DE CAMPO:

Prácticas en Laboratorios: En determinadas unidades se desarrollarán prácticas de laboratorios.

Software Utilizado:

- Vega Scanner
- Autopsy

METODOLOGÍA DE EVALUACIÓN:

Exámenes Parciales

- Existirán dos evaluaciones parciales según lo indicado en el cronograma.
- Las evaluaciones serán escritas y prácticas, pudiendo la cátedra llevar a cabo evaluaciones orales y/o en la PC.
- Los exámenes serán corregidos por los docentes del curso y las notas serán entregadas a los alumnos como máximo a los 7 días hábiles de la toma del parcial.

Examen Final

- 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.
- El primer llamado a examen final será al final del cuatrimestre según cronograma fijado por el Departamento de Ingeniería.
- Las fechas de examen final son fijadas por el Departamento de Ingeniería. Las condiciones de inscripción al final las establece el Departamento de Ingeniería.
- El examen final será confeccionado de forma uniforme para todas las comisiones.
- En fecha de final no se entregan trabajos prácticos.
- En el caso de exámenes libres se confeccionarán de forma especial de manera de evaluar la parte teórica/práctica con el mismo nivel que para alumnos regulares.
- Los exámenes serán corregidos por cualquier docente de la cátedra.

Examen Final Libre

- 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.

CRONOGRAMA ORIENTATIVO DE ACTIVIDADES

Clase	Contenido
1	Introducción a la Seguridad Informática. Ciberseguridad. Ransomware. Ingeniería Social y Ataques Informáticos.
2	Seguridad Física
3	Seguridad Lógica
4	Seguridad en Redes
5	ISO 27001 / ISO 27002
6	Gestión de Riesgos Business Continuity & Disaster Recovery Plan
7	Contratos Informáticos. Licencias. Derecho de Autor y Propiedades.
8	Derecho de Autor y Propiedades.
9	Auditoria de Sistemas. Estándar COBIT. BCRA 4609
10	Protección de Datos Personales. Peritaje Forense Informática. Delitos Informáticos
11	Modalidades de delitos informáticos. Informática Forense e Investigación Digital.
12	Seguridad en el Ciclo de Vida del Desarrollo (SDLC). Introducción a OWASP
13	Penetration testing execution standard (PTEST). Application Security Verification Standard. VEGA.
14	Introducción a la Criptografía. Criptomonedas

CONDICIONES DE CURSADA Y APROBACIÓN

Según lo establecido en la RHCS 054/2011 (Régimen académico integrado)

"Declaro que el presente programa de estudios de la asignatura Auditoria y Seguridad Informática, es el vigente para el ciclo lectivo 2020, guarda consistencia con los contenidos mínimos del Plan de Estudios"

Mg. Ing. Cintia Gioia		*25/03/2020*
Firma	Aclaración	Fecha