1. OBJETIVOS:

a- De la cátedra

Proporcionar a los alumnos el conocimiento general sobre Seguridad y Auditoría Informáticas que requiere todo profesional del área, ya que los temas de esta materia alcanzan a todas las actividades que se realizan con computadoras e información.

Proporcionar una visión integral de Seguridad y Auditoría Informáticas como profesiones para que el alumno que la considere como una posible área de especialización, cuente con los mejores elementos para tomar su decisión.

b- Del alumno

Llevar adelante un aprendizaje teórico-práctico sobre Seguridad y Auditoría Informáticas, por medio de actividades de asistencia a clases e investigación, a partir de las cuales desarrollará un conjunto de trabajos prácticos y evaluaciones.

Adquirir conocimientos sobre Seguridad y Auditoría Informáticas que le permita, sea cual fuere su especialidad y posición dentro del campo profesional, cumplir con los requerimientos de seguridad y auditoría de su entorno y participar de manera proactiva en su desarrollo.

c- Contenidos Mínimos

Conceptos básicos de la Seguridad Informática. Privacidad, integridad y disponibilidad en sistemas informáticos. Organización y control de la Seguridad Informática. Políticas de Seguridad Informática. Seguridad de la gestión de los activos informáticos. Seguridad de los Recursos Humanos. Seguridad de la gestión de las comunicaciones y de las operaciones. Seguridad del control de acceso a los sistemas informáticos. Seguridad en redes. Seguridad en Sistemas Operativos. Seguridad en bases de datos. Seguridad en transacciones y sistemas distribuidos. Elementos de Criptografía, sistemas simétricos y asimétricos, certificados digitales y firma digital. Seguridad física y ambiental. Seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos. Seguridad en el desarrollo de software. Seguridad en la gestión de los incidentes de seguridad de la información. Seguridad en la gestión de la continuidad del negocio, planes de contingencia continuidad y recuperación. Auditoría de Seguridad Informática. Elementos de peritaje informático e informática forense. Cumplimiento del marco legal, reglamentario y normativo de la Seguridad Informática.

2. Contenidos:

La Cátedra de Seguridad y Auditoría Informática fue estructurada para que los Alumnos desarrollen las siguientes bases conceptuales y prácticas.

Organización y Control (Unidad 2)
Criptografía (Unidad 3)
Seguridad Física y Ambiental (Unidad 4)
Continuidad de los Negocios (Unidad 5)
Auditoría (Unidad 6)
Cumplimiento (Unidad 7)

Unidad I: Conceptos Básicos

1. La Seguridad Informática como una de las Ciencias de la Computación.
2. El paradigma de la Seguridad Informática. Confidencialidad, Integridad y Disponibilidad en sistemas informáticos.
3. Conceptos y terminología básicos.

Unidad II: Organización y control de la Seguridad Informática

1. Políticas de Seguridad Informática.
2. Seguridad de la gestión de los activos informáticos.
3. Seguridad de los Recursos Humanos.
4. Seguridad de la gestión de las comunicaciones y de las operaciones.
5. Seguridad de los controles de acceso a los sistemas informáticos.
6. Seguridad en redes.
7. Seguridad en Sistemas Operativos.
8. Seguridad en bases de datos.
9. Seguridad en transacciones y sistemas distribuidos.
10. Seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos.
11. Seguridad en el desarrollo de software.
12. Seguridad en la gestión de los incidentes de seguridad de la información.

Unidad III: Elementos de Criptografía

1. Sistemas simétricos
2. Sistemas asimétricos. Modelo de Diffie y Hellman.
3. Algoritmos Simétricos y Asimétricos estándar.
4. Criptografía aplicada al Control de Integridad. Algoritmos Hash
5. Certificados digitales
6. Firma electrónica
7. Firma digital
8. Sistemas de transacciones financieras.

Unidad IV: Seguridad Física y Ambiental

1. Perímetros de Seguridad
2. Controles de acceso físico
3. Protección contra amenazas externas y del ambiente

4. Trabajo en áreas protegidas
5. Seguridad, mantenimiento, logística y baja del equipamiento.

Unidad V: Seguridad en la gestión de la continuidad del negocio.

1. Planes de Contingencia
2. Planes de Continuidad de Negocio
3. Planes de Recuperación de Desastres. Centros de Cómputos Alternativos. Centro de Cómputos de Alta Seguridad
4. Pruebas de los Planes
5. Documentación de los Planes y sus Procedimientos.

Unidad VI: Auditoría de Seguridad Informática

1. Rol de la Auditoría de Seguridad Informática.
2. Auditorías Internas, Externas y Cruzadas.
3. Elementos de peritaje informático e informática forense.

Unidad VII: Cumplimiento.

1. Cumplimiento del marco legal. Ley de Firma Digital, Ley de Protección de Datos Personales, Ley de Delito Informático. Cumplimiento de la Reglamentación de la las Leyes.
2. Cumplimiento de marco normativo. Familia de normas IRAM-ISO
3. Cumplimiento del marco regulatorio. Circulares del Banco Central de la República Argentina.

3. BIBLIOGRAFIA

3.1. Primaria

Enciclopedia de la Seguridad Informatica, Gomez Vieites Alvaro, Editorial Alfaomega Grupo Editor

Criptografía, Técnicas de Desarrollo para Profesionales, Maiorano Ariel, Editorial Alfaomega Grupo Editor

Hackers al Descubierto, Entienda sus Vulnerabilidades evite que lo Sorprendan, Pacheco Federico G. Jara Hector, Editorial Gradi

Ethical Hacking, Pacheco Federico G. Jara Hector, Editorial Gradi

3.2. Secundaria

Computación Forense, Descubriendo Los Rastros Informáticos, Cano Martinez Jeimy J., Editorial Alfaomega Grupo Editor

Peritajes Informaticos, Del Peso Navarro Emilio, Editorial Diaz De Santos

La Seguridad de los Datos de Caracter Personal, Del Peso Navarro Emilio Ramos Gonzalez Miguel A., Editorial Diaz De Santos

El Arte de la Intrusion, Mitnick Kevin D., Editorial Alfaomega Grupo Editor

3.3. Consulta

Fundamentos de Seguridad en Redes, Stallings William, Editorial Pearson Alhambra

4. METODOLOGIA DE LA ENSEÑANZA

El alumno deberá asistir conjunto de Actividades que le permitirán conformar su entorno de aprendizaje, las cuales se desarrollarán en los siguientes lugares:

a. Actividades de Enseñanza en el Aula. Clases Grupales de tipo Teórico.
b. Actividades de Práctica en Laboratorios de Computadoras, que le permitirán familiarizarse con el ambiente de trabajo, y desde allí construir en la operación su Aprendizaje.
c. Actividades de Investigación aplicada en los Trabajos Prácticos, de tipo Grupal. Cada Investigación deberá concluir con la correspondiente **presentación de la documentación** escrita y con el correspondiente medio de almacenamiento (disquette – cd – dvd). En todos los casos la funcionalidad es la base de la corrección y aprobación de la asignatura.

Lo anterior será posible materializarlo con trabajos de investigación, desarrollo de aplicaciones y evaluaciones de tipo Individual y Grupal.

Esto permitirá al alumno:

Adquirir vocabulario técnico-informático y utilizarlo con precisión
Conocer las funciones de la Seguridad Informática en una organización.
Evaluar, a nivel de implementación, herramientas básicas de Seguridad Informática.
Desarrollar capacidades de investigación utilizando publicaciones, libros y analizando elementos reales existentes.
Desarrollar la capacidad de detectar riesgos informáticos en organizaciones y poder aportar conceptos para su solución.

Los Alumnos además deberán desarrollar una serie de Trabajos de Investigación, con formato predefinido, en los cuales se desarrollarán temas concernientes a los vistos en Aula, y deberán ser entregados, con una frecuencia de 15 días. Los temas son:

Utilización de la Ingeniería Social en los Ataques Informáticos
Conveniencia de implementar Firma Digital o Firma Electrónica
Conveniencia de utilizar Protocolos Criptográficos Estándar o Propietarios
Conveniencia de implementar el Modelo de Sala Cofre o de Centro de Cómputos Alternativo

Todos los ensayos deben declarar bibliografía y otras fuentes. El contenido textual de terceros no pueden superar el 30% del escrito.

Detalle de Actividades prácticas

Lo anterior será posible materializarlo con trabajos de investigación, desarrollo de aplicaciones y evaluaciones de tipo Individual y Grupal. Estas pueden listarse de la siguiente forma:

Formación experimental (P1)

Se resuelven problemas que ilustran la teoría mediante ejemplos que se plantean en el pizarrón y luego se resuelven mediante las herramientas seleccionadas. Los problemas

ofrecen dificultades crecientes y en algunos casos son versiones simplificadas de problemáticas reales.

Problemas Abiertos de Ingeniería (P2)
Son problemas que corresponden a situaciones reales o hipotéticas cuya solución requiera la aplicación de los conocimientos de las ciencias básicas y de las tecnologías utilizadas en la Seguridad Informática. En general no tienen un planteo matemático único, sino que dependerá de los requerimientos de los que toman las decisiones y los límites que pueden plantearse a la complejidad. Las conclusiones deben presentarse en informes grupales, que deben resultar útiles a quien tome decisiones en el diseño e implementación de los Sistemas de Seguridad y/o Auditoría Informática.

Prácticas de proyecto y diseño de sistemas informáticos(P3)
Se entiende por tales a las actividades que empleando ciencias básicas y de la ingeniería llevan al desarrollo de un sistema, componente o proceso, satisfaciendo una determinada necesidad y optimizando el uso de los recursos disponibles. Corresponde a los casos más complejos planteados, donde los alumnos deben relacionar conceptos de matemática, economía, sistemas y toma de decisiones. Las conclusiones deben presentarse en informes grupales, que deben resultar útiles a quien tome decisiones.

Instrucción Supervisada de Formación Práctica (P4)
Se entiende por tales a las actividades que empleando diversas herramientas de software y hardware permiten conformar un conocimiento práctico, aplicable al ámbito profesional. Son actividades grupales y se realizan en forma concentrada en los Laboratorios, guiados por el Docente.

Conformación de los Trabajos Prácticos a realizar por los Alumnos a lo largo de su cursada.

Unidad temática	Trabajo Práctico
I: Conceptos Básicos	**TP1: Análisis de la evolución del Paradigma de la Seguridad Informática**
II. Organización y control	**TP2: Desarrollo de una Política de Seguridad Informática**
III. Elementos de Criptografía	**TP3: Instalación y uso de un Sistema de Correo Electrónico Encriptado**
IV: Seguridad Física y Ambiental	**TP4: Investigación sobre el concepto de Sala Cofre.**
V: Seguridad en la gestión de la continuidad del negocio	**TP 5 Desarrollo de un Plan de Contingencias**
VI: Auditoría de Seguridad Informática	**TP 6 Instalación y uso de un Intrusion Detection Systems**
VII: Cumplimiento	**TP 7: Investigación sobre el impacto del marco legal en una organización**

5. CRITERIOS DE EVALUACION

La evaluación de los alumnos se realiza a través de Trabajos Prácticos (TPs), participación en clases, evaluaciones parciales y el Examen Final.

En los TPs: los alumnos deberán poner en juego las competencias desarrolladas y los conocimientos adquiridos mediante la resolución de problemas. Se tomarán en cuenta el contenido, el cumplimiento de objetivo y consignas y la calidad de la presentación (prolijidad, ortografía, comunicación).

En la participación en clase: Los alumnos serán evaluados en forma permanente a través de la calidad y oportunidad de sus intervenciones.

***En los Parciales*:** la evaluación parcial tiene como objetivo corroborar el aprendizaje realizado por los alumnos durante el curso y su evolución. Se verificará el nivel de cumplimiento de los objetivos pedagógicos del curso.

En el Examen Final: La evaluación final estará basada sobre la examinación del conocimientos vistos en la materia y resolver problemas reales que permitan poner en evidencia la integración de conocimientos. Se verificará la capacidad de los alumnos en la utilización de los conceptos fundamentales de la asignatura para la organización de su trabajo, así como el nivel de análisis desarrollado y la calidad de la solución propuesta.

5.2 Requisitos para la aprobación

Aprobación del cursado de la asignatura. Para aprobar es necesario cumplir con:

Asistencia mínima del 50%

Aprobación del examen parcial con nota igual o superior a cuatro puntos:

Los parciales deben rendirse en las fechas estipuladas por la Facultad, según cronograma general de la Universidad.

En el caso de que el alumno desapruebe el examen parcial cuenta con una instancia de recuperación.

El desaprobar o no asistir a la recuperación (teniendo el parcial desaprobado) tiene como consecuencia desaprobar el curso de la materia.

Aprobación de los Trabajos prácticos con nota igual o superior a cuatro puntos:

En el caso de esta materia la nota final de los trabajos prácticos se calcula como una nota promedio de los trabajos requeridos que equivale al 75% del número de TPs obligatorios.

Aprobación de la asignatura. Para aprobar la materia es necesario aprobar el cursado y el Examen Final

Para aquellos alumnos que no alcanzaran el 75% de asistencias deberán rendir un Examen Final Escrito y luego un Examen Final Oral.

Para los alumnos que alcancen o superen el 75% el Examen Final será sólo te tipo Oral.