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.

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. Segundaria

- 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. Estas son:

- **Practicas de Resolución de problemas**
- **Practicas de Laboratorio**
- **Practicas de Simulación**
- **Practicas de Diseño y Proyecto**
- **Presentaciones de temas específicos por Alumnos.**
- **Trabajos de Campo**

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

Unidad temática	Trabajo Práctico	Res. Probl	P.Lab	Pr. Simul.	Pr. Dis. Y Proy.	Trab. Campo	Hs.
I: Conceptos Básicos	**TP1: Análisis de la evolución del Paradigma de la Seguridad Informática**	50%	0%	0%	0%	50%	6hs
II. Organización y control	**TP2: Desarrollo de una Política de Seguridad Informática**	40%	0%	20%	20%	20%	12hs
III. Elementos de Criptografía	**TP3: Instalación y uso de un Sistema de Correo**	30%	70%	0%	0%	0%	6hs

	Electrónico Encriptado						
IV: Seguridad Física y Ambiental	**TP4: Investigación sobre el concepto de Sala Cofre.**	50%	0%	0%	0%	50%	6hs
V: Seguridad en la gestión de la continuidad del negocio	**TP 5 Desarrollo de un Plan de Contingencias**	40%	0%	20%	20%	20%	6hs
VI: Auditoría de Seguridad Informática	**TP 6 Instalación y uso de un Intrusion Detection Systems**	30%	70%	0%	0%	0%	6hs
VII: Cumplimiento	**TP 7: Investigación sobre el impacto del marco legal en una organización**	40%	0%	20%	20%	20%	6hs
					Total Hs Prácticas		**48hs**

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.

5. CRITERIOS DE EVALUACION

La evaluación final está compuesta por:
Evaluación Diagnóstica.
Evaluaciones por clase
Un examen parcial y un examen Recuperatorio (para el caso de no aprobación del primero) con fecha determinada por cronograma general de la Universidad.
Trabajos prácticos (individuales y por grupos de 2 o 3 alumnos).
Trabajos de Investigación (individuales)
Examen Final

6. AUTORIDADES DE LA UNIVERSIDAD DE BELGRANO

Dr. Avelino Porto Presidente
Dr. Eustaquio Castro Vicepresidente de Gestión Técnica y Administrativa
Prof. Nilda V. de Brigante Vicepresidente de Docencia e Investigación
Prof. Aldo J. Pérez Vicepresidente de Gestión Institucional

7. AUTORIDADES DE LA FACULTAD DE INGENIERIA.

Ing. Alberto Guerci – Decano.
Lic. Paula Angeleri – Director de Carrera.
Ing. Sergio Omar Aguilera - Coordinador