UNIVERSIDAD DE MENDOZA – FACULTAD DE INGENIERÍA

CARRERA INGENIERIA EN INFORMATICA	ASIGNATURA Seguridad Informática I	CÓDIGO 2044
CURSO 4to AÑO	ÁREA TA	ULTIMA REVISIÓN 2008
MATERIAS CORRELATIVAS:		AÑO LECTIVO 2012

Profesor Titular: Lic. Rolando Conde
Profesor Asociado: Ing. Carlos Tomba
Profesores Adjuntos:
Jefes de trabajos prácticos:

Carga Horaria Semanal: 5 hs.
Carga Horaria Total: 75 hs.

OBJETIVOS:

Conocer y comprender el alcance de los conceptos de Seguridad Integral de los Sistemas Informáticos. Interpretar, analizar e implementar los estándares internacionales de la Seguridad Informática.- Poder determinar los valores y costos de la implementación de un plan de seguridad.- Realizar un Análisis de Riesgos Informáticos.- Poder definir un plan de Contingencia del Negocio.

PROGRAMA ANALÍTICO:

Unidad 1.- Introducción al tema de Seguridad

1.1 Antecedentes
1.2 Caracteristicas: 1.2.1 Integridad 1.2.2 Confidencialidad 1.2.3 Disponibilidad
1.3 Objetivos 1.3.1 Elementos a Proteger 1.3.2 Términos y Conceptos relacionados con la Seguridad
1.4. La información. 1.4.1. La información y su necesidad de ser protegida.
1.5 Que es la seguridad de la información. 1.5.1. Los sistemas de información desde el punto de vista de la seguridad.
1.6 Costos de la seguridad de la información. 1.6.1 Alcance y costos de la seguridad de la información. 1.6.2 Relación entre la operatividad y la seguridad. 1.6.3. Como establecer los requerimientos de seguridad.

Unidad 2.- Riesgos

2.1 Introducción 2.2. Definición de Riesgos 2.3 Conceptos: Probabilidad, Amenazas, Vulnerabilidades, Activos, Impactos

2.4 Administración del Riesgo 2.4.1. Análisis de Riesgos 2.4.2 Identificar Activos 2,4,3 Identificar Amenazas 2.4.4 Determinación del Impacto 2.4.5 Determinación del Riesgo 2.4.6 Salvaguardas 2.4.7 Riesgo Residual
2.4.8 Matriz de Riesgos

Unidad 3.- Seguridad Fisica

3.1 Seguridad Física 3.1.2. Perímetro de Seguridad 3.1.3.Controles de Acceso 3.1.4 Copias de Seguridad 3.1.5 Suministro de Energia-UPS 3.1.6 Cableados 3.1.7 Mantenimiento de Equipos . 3.1.8 Disposición, Refrigeración y Mantenimiento del equipamiento 3.1.9. Protecciones contra incendios.

Unidad 4.- Seguridad Lógica

4.1 Seguridad Lógica 4.1.1 Seguridad en Capas 4.1.2.Subdivisión en zonas.
4.1.3 Componentes de seguridad (Firewall, gateway antivirus, etc.)
4.2.1 Detección de Intrusos 4.2.2 Detección de Vulnerabilidades
4.3.1 Seguridad Integrada 4.3.2 Capa de Redes 4.3.3 Subdivisión de redes
4.3.4 Control de acceso, política de password, gestión de privilegios, certificados digitales, caminos forzados, recursos compartidos 4.3.5 Control de tráfico y vulnerabilidades. 4.3.6 Capa de Aplicaciones.
4.4.1 Ambiente de desarrollo y producción 4.4.2.Resguardo de la información, políticas de backup.
4.5.1 Componentes de seguridad (Firewall de aplicación, VPN, Control de contenidos, Antivirus , Gateway de http-smtp, etc.).
4.6.1 Capa de Host. Componentes de seguridad (Arreglo de discos, Antivirus, IDS, Anti spyware.-

Unidad 5 Seguridad Administrativa y Legal

5. 1 Seguridad Administrativa y legal 5.2 Política de Personal
5.3 Politica de Seguridad de la Empresa
5.4 Ley de Habeas Datas 5.5 Firma Digital 5.6 Propiedad Intelectual 5.7 Confidencialidad
5.8 Contratos Informáticos

Unidad 6 : Metodología de Análisis y Gestión de Riesgos – MAGERIT

6.1 Evaluación y Gestión de Riesgos. 6.1.2 Elemento de una Matriz de Riesgo, 6.1.3 Fases de Construcción de una Matriz.- 6.1.5 Metodología de Supervisión.
6.1.6 Tipos de activos, 6.1.7 Dimensiones de valoración, 6.1.8 Criterios de valoración, 6.1.9 Amenazas, 6.1.10 Salvaguardas

Unidad 7: Gestión de la continuidad de negocio

7.1 Continuidad del negocio y el análisis del impacto. 7.1.2 Diseño e implementación de planes de contingencias. 7.1.3 Prueba, mantenimiento y reevaluación de los planes de contingencia.

Unidad 8: Sistema de Gestión de la Seguridad Informática SGSI ISO 27001

8.1 Que es un SGSI 8.2 Para que sirve un SGSI 8.3 Que incluye un SGSI
8.3.1 Documentación de los Niveles 1,2,3 y 4.- 8.4 Como se Implementa un SGSI
8.4.1 Plan: Establecer el SGSI 8.4.2 Do: Implementar y utilizar el SGSI
8.4.3. *Check:* Monitorizar y revisar el SGSI 8.4.4. *Act:* Mantener y mejorar el SGSI
8.5 tareas de la Gerencia en un SGSI 8.6 Compromiso de la dirección
8.7 Revisión del SGSI 8.8 Certificación 8.9 Documentacion

Formación Práctica	Horas
Resolución de Problemas Rutinarios:	
Laboratorio, Trabajo de Campo:	
Resolución de Problemas Abiertos de ingeniería:	25 hs.
Proyecto y Diseño:	

PROGRAMA DE TRABAJOS PRÁCTICOS:

Trabajo Práctico N° 1: Matriz de Riesgo
Trabajo Práctico N° 2: Plan de Contingencia del Negocio
Trabajo Práctico Nº 3: Anáisis de Activos Informáticos

ARTICULACIÓN HORIZONTAL Y VERTICAL DE CONTENIDOS:

- Los contenidos abordados en esta materia se basan en conceptos de las siguientes cátedras:

Asignatura	***Curso***
Análisis de Sistemas	3ero
Diseño de Sistemas	3ero
Computación	2do

- Comparte e integra elementos horizontalmente con las siguientes cátedras:

Asignatura	***Curso***
Organización	4to

- Los contenidos abordados en esta materia aportan conceptos a las siguientes cátedras:

Asignatura	***Curso***
Auditoria de Sistemas	4to

CONDICIONES PARA REGULARIZAR LA MATERIA y RÉGIMEN DE EVALUACIÓN:

El alumno debe cumplir
Clases de Desarrollo Teórico 80% de asistencia.
Talleres Prácticos 100% de asistencia.
Evaluaciones Parciales aprobadas con el 60%.

ESTRATEGIAS DIDÁCTICAS UTILIZADAS:

- Clases expositivas
- Trabajos teórico - prácticos grupales e individuales
- Trabajos prácticos individuales
- Visitas realizadas a diversas Instalaciones
- Exposiciones de Instalaciones por medio de documentación fotográfica y documentos en PDF, PowerPoint, etc.

BIBLIOGRAFÍA:

Principal:

Autor	Título	Editorial	Año Ed.
Claudia Bello	Manual de Seguridad	Adm.Pública Nacional	Disponible en la Cátedra
Jefatura de Gabinete	Modelo de Política de Seguridad de la Información para los Organimos de la Administración Pública	Adm.Pública Nacional	Disponible en la Cátedra
Lic. Javier Diaz, Lic.Paubla Venosa	Seguridad de las Organizaciones, fortalezas y debilidades de la Norma ISO 27001/2	Versión Digital	

De Consulta:

Autor	Título	Editorial	Año Ed.
ISO/OSI	Norma ISO 27001/2,	ISO/OSI	
Gobierno Español -	Magerit Versión 2 Mertodología de Analisis y Gestión de Riesgos	Gob.Español	Disponible en la Cátedra
Nando ABC	Seguridad en Sistemas	Versión	

	de Información	Digital	
Chelo Poyato, Francisco Coll, David Moreno	Recomendaciones de Seguridad	Versión Digital	
Instituto IRIS-CERT Certrediris.es	Recuperación ante ataques	Versión Digital	
Las diez Vulnerabilidades De seguridad en internet más críticas	The Sans Institute	Versión Digital	

ESTRATEGIAS DIDÁCTICAS UTILIZADAS:

- Clases expositivas
- Trabajos teórico - prácticos grupales e individuales
- Trabajos prácticos individuales

RECURSOS DIDÁCTICOS UTILIZADOS:

- Textos
- Pizarrón y tiza
- Transparencias
- Guías de trabajos prácticos
- Apuntes elaborados para consulta de los alumnos

PROGRAMA DE EXAMEN:

Examen Oral
Programa analítico completo abierto.-