Departamento Ingeniería en Sistemas de Información

ASIGNATURA:	SEGURIDAD INFORMÁTICA
DEPARTAMENTO:	ING. EN SIST. DE INFORMACION
AREA:	ELECTIVA
BLOQUE	COMPLEMENTARIAS

MODALIDAD:	Cuatrimestral
HORAS SEM.:	4 horas
HORAS/AÑO:	64 horas
HORAS RELOJ	48
NIVEL:	3º
AÑO DE DICTADO:	Plan 2008

Objetivos

- Desarrollar una actitud crítica y reflexiva con respecto a la seguridad en la organización.
- Proporcionar la necesidad de la seguridad en las organizaciones en el área de seguridad de la información.
- Comprender los distintos aspectos de la seguridad informática, necesarios en las organizaciones.
- Reconocer los principales sectores funcionales en las organizaciones y sus particulares requerimientos de seguridad y puntualmente la seguridad en la información.
- Incorporar las herramientas necesarias para el control de la seguridad en la información de las organizaciones y la coordinación de sus distintos sectores.

Contenidos Mínimos (Programa Sintético).

- Introducción a los conceptos genéricos de la seguridad en informática. Su necesidad. Riesgos y amenazas. Seguridad física, lógica y administrativa.
- Nociones de auditoria informática a fin de posibilitar contar con herramientas que posibiliten determinar los niveles de seguridad de una instalación.
- Organización del área de seguridad informática en una empresa interactuando con todo el espectro de la seguridad y sin dejar de lado el factor humano y los aspectos legales.
- Poder detectar las vulnerabilidades de los sistemas informáticos
- Implementar Estructuras Preventivas y Disuasivas Planes de contingencia y continuidad de negocios.

Contenidos Analíticos:

Unidad I

Introducción a la seguridad. Definición, terminología y conceptos: Seguridad, Riesgo, Vulnerabilidad, Análisis de Riesgo, Plan de Contingencia, Plan de Continuidad de Negocios. Los riesgos en la información a través del tiempo.

Unidad II

Políticas y Normas de Seguridad. Valorización del bien a proteger. Clasificación de la Información. Metodologías de Análisis de Riesgo. Cuantitativa, Cualitativa, Mixta, beneficios y vulnerabilidades. Control y Auditoria en la gestión de Seguridad.

Unidad III

Factor Humano en la Seguridad de la Información. Selección y Políticas para el Personal. Estructuración de la actividad en áreas de manejo de información (asignación de tareas, control por oposición, capacitación, estandarización, etc.). Pacto de Confidencialidad. Encriptación. Firmas digital y electrónica. Ingeniería social y espionaje, metodologías. Redes Sociales - Generación X Y

Unidad IV

Estructura Edilicia en áreas de sistemas, riesgos perimetrales, zonas restringidas. Control de accesos a las áreas de sistemas sus riesgos y vulnerabilidades. Selección y uso componentes de seguridad electrónica. Riesgos eléctricos e incendios en centros de procesamiento de información. Normativas de prevención. Tipos de extintores y de fuego. Resguardo del equipamiento informático.

Unidad V

Estructura de los sistemas informáticos administrativos contables, vulnerabilidades que pueden presentar para el fraude. Desarrollo Seguro - Metodología OWASP. Vulnerabilidades en los vínculos de comunicación. Integridad y robustez de los sistemas informáticos.

Unidad VI

Programación y accionar dañino. Distintos tipos (virus, gusanos, zombis, phising, etc). Tipos de ataque a sistemas de información- explotación y laboratorio (herramientas utilizadas). Accionar y Software vigente para disminuir los riesgos y vulnerabilidades enunciados en esta unidad.

Unidad VII

Leyes, regulaciones y Compliance (ISO 2700x, SOX, sas70, Pci, circulares BCRA). Ley de Delitos Informáticos. Informática Forense. Indicio y Prueba en un Delito Informático, recolección y resguardo de los mismos. La evaluación de los indicios, rastros y pruebas informáticas, herramientas y metodología para realizarlas.

Bibliografía.

- Se considera una **bibliografía básica** para el desarrollo de las actividades de la materia seguridad informática la siguiente:
- Normas ISO/ IRAM 2700x o la que resulte vigente en el momento del dictado con respecto al manejo seguro de informática
- Recopilación de Normas del Banco Central de RA sobre requisitos Operativos Mínimos para el área de Tecnología al año 2009
- NORMA IRAM 17550 Sistema de Gestión de Riesgo o la vigente en el momento del dictado
- Lic. Juan C. Tirante - 2009 3ra Edición - Delitos Informáticos de ayer y de hoy, su análisis - Editorial Centro de Estudiantes de FRBA
- Suscripción a http://www.hispasec.com/ sitio de la Web sobre seguridad informática que brinda una noticia al día sobre actualidad al respecto.
- ***Bibliografía de Consulta****:*
- Fernando Picouto Ramos, Antonio Ángel Ramos- 2008 1ra Edición -Hacking y Seguridad en Internet - Editorial Alfaomega - México
- Federico Pacheco - 2009 1ra Edición - Hacker al Descubierto Argentina - Editorial USERS
- Mario G. Piattini - 2005 2da Edición - Auditoria Informática un Enfoque práctico - Editorial Alfaomega Editado - Colombia
- Randall K. Nichols - 2006 2da Edición - Seguridad para las comunicaciones inalámbricas - MC Graw Hill - España Barcelona.

Correlativas

Para Cursar:

Cursadas:

- Análisis de Sistemas
- 3 (tres) materias del 2º nivel (además de la anterior)

Para rendir:

Aprobadas:

- Análisis de Sistemas
- 3 (tres) materias del 2º nivel (además de la anterior)