UTN.BA
DEPARTAMENTO
INGENIERIA EN SISTEMAS DE INFORMACION

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:	2018

.

Objetivos

- Desarrollar una actitud crítica y reflexiva con respecto a la seguridad en la organización.
- Adquirirla capacidad de evaluar la necesidad y tipo de seguridad a implementar en el área de información de las organizaciones.
- Comprender los distintos aspectos de la seguridad informática, necesarios en las organizaciones.
- Tener la capacidad de reconocer los principales sectores funcionales en las organizaciones, sus particulares requerimientos de seguridad y puntualmente en la seguridad informática.
- Adquirir 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 sistémica y puntualmente 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 organización, empresa y/o institución, interactuando con todo el espectro de la seguridad, incluyendo la seguridad electrónica, 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

Conceptos básicos de seguridad: Confidencialidad - Integridad – Disponibilidad Identificación - Autenticación - Autorización - Responsabilidad (accountability) - Privacidad - No Repudio (validación de identidad) - Principio de separación de tareas - Mínimo Privilegio - Rotación de tareas. La Pirámide del Plan de Seguridad. Seguridad, Riesgo, Vulnerabilidad, Análisis de Riesgo, Plan de Contingencia, Plan de Continuidad de Negocios. Los riesgos y sus recurrencias 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. Tipos de control de acceso Implementación del Control de Acceso Identificación , Autenticación, Autorización y Auditoría Técnicas de identificación y autenticación Doble factor de autenticación Autenticación basada en comportamiento Protección criptográfica de credenciales Protocolos de autenticación Kerberos Modelos de Control de Acceso Administración de Control de Acceso Monitoreo, Auditoría y Logs Sistemas de Detección de Intrusos Métodos de ataque.

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

Criptografía: Historia de la criptografía.Conceptos Generales.Tipos de algoritmos Cifrado simétrico. Cifrado asimétrico Funciones de Hash de los sistemas informáticos.,Deep Web. Encriptación, características y protocolos que usan encriptación, características de la firma digital

Unidad VI

Malware. Tipos de Malware (virus, gusanos, zombis, phising, etc) y dispositivos vulnerables a los mismos (PC, Celular, Tablet, etc) Tipos de ataque a sistemas de información- explotación y laboratorio (herramientas utilizadas). Accionar, Software y Hardware 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 Obligatoria

- 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 2012
- NORMA IRAM 17550 Sistema de Gestión de Riesgo o la vigente en el momento del dictado
- Lic. Juan C. Tirante - 2012 4ra 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 Complementaria

- Fernando Picouto Ramos, Antonio Ángel Ramos- 2008 1ra Edición -Hacking y Seguridad en Internet - Editorial Alfaomega - México
- Federico Pacheco - 2012 3ra 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
- Sintaxis y Semántica del Lenguaje
- Paradigmas de Programación

Para Rendir:

Aprobadas:

- Análisis de Sistemas
- Sintaxis y Semántica del Lenguaje
- Paradigmas de Programación