Programa de la Asignatura:

Seguridad Informática

Código: 772

Carrera: ***Ingeniería en Computación*** Plan: ***2008*** Carácter: ***Obligatoria***
Unidad Académica: ***Secretaría Académica*** Curso: ***Cuarto Año – Primer cuatrimestre***
Departamento: ***Ingeniería*** Carga horaria total: ***90 hs.*** Carga horaria semanal: ***6 hs.***
Formación Experimental: ***10 %*** Formación teórica: ***70 %*** Formación práctica: ***20 %***

Materias Correlativas Obligatorias

- ***Física III (cód. 750)***
- ----------
- ----------

Cuerpo Docente

Langdon, Roberto

Índice

AÑO ACADÉMICO 2013 ÚLTIMA REVISIÓN 12/04/2013

Firma Docente Firma Coordinador

1. **FUNDAMENTACION**

Esta asignatura está incluida en un grupo de materias, que se ocupa de brindar conocimientos en el área de las tecnologías de las ciencias de la computación y las telecomunicaciones.

El desarrollo rápido y la evolución constante de los ataques de seguridad informática, contra sistemas computacionales, redes, infraestructuras edilicias, junto con los incidentes de seguridad física que pueden sufrir organizaciones e individuos, justifica plenamente la necesidad de capacitar a los alumnos en el manejo de las diversas técnicas de protección de los activos de información, sus sedes, y sus individuos.

El desarrollo de las capacidades necesarias para la selección de distintas opciones, permitirá que en las organizaciones donde estará inserto el futuro egresado, encuentre a un profesional dotado de estos conocimientos tan necesarios para proteger, salvaguardar e impedir que los diversos tipos de ataque de seguridad, cada vez más sofisticados, dañinos pero al mismo tiempo simples de ejecutar, puedan provocar pérdidas de información, daños a terceros, la comisión de delitos en tecnología, y la garantía de continuidad de las operaciones.

Conocer las distintas herramientas, saber como implementar políticas de seguridad, y asistir a sus organizaciones en la disciplina de Seguridad de la Información, le permitirá ser un factor de gran valor agregado para su organización, al mismo tiempo que para su comunidad y familia.

El alumno se formará con una escala de valores éticos, criterios de moral y ética profesional.

2. **ENCUADRE Y ARTICULACIÓN DE LA ASIGNATURA**

Encuadre dentro del Plan de Estudios

La asignatura está ubicada en la currícula de la carrera en la parte final de la misma que corresponde al "Ciclo Profesional".

En esa etapa, los alumnos ya han adquirido bastante experiencia en el uso del computador como herramienta para el manejo de la información.

Requiere una sólida formación en redes, sistemas operativos, y operaciones informáticas.

Articulación Horizontal

Al pertenecer a materias de 4° año, el alumno se encuentra en una estapa de tener acceso a conocimientos específicos sobre su especialidad, donde podrá sumar experiencias al contar con materias tales como Ingeniería en Software donde la disciplina de programación segura podrá apalancarse, de la misma manera que con las materias de Procesamiento de Imágenes, dado a que podrán conocer técnicas que luego servirán para entender los objetivos de la Esteganografía.

Articulación Vertical

Materias de 5° año tales como Auditoría de Sistemas, que tiene como correlativa a Seguridad Informática, es una de las asignaturas críticas de la especialidad y de la carrera, porque contará con los conocimientos y herramientas, para sumar a la disciplina de auditoría de sistemas, a fin de ser acertivos en sus investigaciones, verificaciones y comprobaciones.

Y todo lo relacionado con Informática Médica, y con Sistemas de Adquisición de Datos, esta materia de Seguridad Informática les habrá dejado los conceptos de protección de datos sensibles y privados, las

técnicas existentes para intentar violar sus políticas de protección de datos, y las maneras de contrarrestarlo.

3. **OBJETIVOS**

Objetivo General

Formar el concepto de Seguridad de la Información, en sus diversos aspectos, centrando el objetivo en la Confidencialidad de los datos, la Integridad de los Datos, y la Disponibilidad de los datos, y sus correspondientes relaciones en virtud de la generación de información, y el valor que ésta tiene para las organizaciones como su principal activo a proteger.

Objetivos Específicos

1. Introducir al alumno en los fundamentos de la Seguridad de la Información
2. Conocer los distintos tipos de ataques y metodologías de desarrollo
3. Brindar conocimientos sobre los distintos componentes básicos en la protección de la información, ya sean de seguridad informática como de seguridad física
   i. Protección Física - Seguridad Patrimonial
   ii. Protección Informática - Seguridad de Redes Teleinformáticas
4. Introducir los conceptos de criptografía y su aplicación práctica en el campo
5. Introducir los conceptos de Seguridad en Telecomunicaciones
6. Introducir los conceptos de Seguridad Física que permitan al alumno diseñar soluciones acorde a la necesidad de la empresa de proteger sus activos de información
7. Transmitir los conocimientos necesarios para la realización de un Plan de Continuidad de Negocios
8. Dar a conocer la legislación nacional e internacional en materia de delitos informáticos que permita al alumno interactuar y asesorar al área de Legales de la empresa en la que se desempeñe.
9. Generar conciencia sobre los peligros a los que están expuestos los empleados de una compañía a partid de la utilización de las técnicas de Ingeniería Social para obtener información
10. Transmitir los conocimientos básicos sobre la norma ISO/IEC 27002 y su utilidad para el desarrollo del Plan de Seguridad de la Empresa.

4. **CONTENIDOS MÍNIMOS**

Conceptos básicos: Criptografía y Criptoanálisis. Criptografía clásica y Criptografía moderna. T,cnicas básicas: Cifrado-decifrado y firma. Criptografía de clave privada y de clave publica. T,cnicas modernas de clave privada: Cifrado en bloque. La norma DES. Criptoanálisis. Variantes del DES. Otros cifrados bloque. Combinaciones de cifradores. Cifrados flujo (stream) Funciones hash one-way. Cifrados de clave pública. Firma Digital. Protocolos criptográficos: Introducción a protocolos. Comunicaciones utilizando claves públicas. Firmas digitales. Intercambio de claves. Autenticación. Servicios de registro de tiempo. Firmas. Protocolos avanzados. Conceptos básicos de seguridad. Seguridad en Sistemas operativos (UNIX, Windows NT). Listas de Control de Acceso. Seguridad del Sistema de Archivos. Control de Acceso. Buffer Overflow. Race Condition. Cuentas y su defensa. Auditoria. Seguridad en redes e Internet: Redes TCP/IP. Seguridad en WWW. Firewalls. Wrappers y proxies Problemas de Implementación del TCP/IP. Ataque típicos. One Time Passwords. Single Sign On. Criptografía cuántica.

5. **PROGRAMA ANALÍTICO**

UNIDAD 1: Fundamentos de Seguridad de la Información

- Qué es la Seguridad de la Información
- Importancia y Valor de la Información
- Estadísticas de la Inseguridad
- Perfil de los potenciales atacantes

- Tipos de Ataques
- La Ingeniería Social
- Objetivos de la Seguridad de la Información - CIA
- La Seguridad como Proceso Contínuo
- Riesgos ante la ausencia total o parcial de Políticas de Seguridad de la Información

UNIDAD 2: Protección de Redes Teleinformáticas

- Concepto de Antivirus y AntiSpywares - Ejercitación con productos de Antivirus y AntiSpywares – Desinfección de PC's (ESET, Kaspersky, AVG, AVAST, Spybot Search & Destroy, SuperAntispyware, Spywareblaster, IOBIT Advanced System Care, etc)
- Concepto de Antispam y AntiPhishing - Ejercitación con productos de Antispam (SpamTitan, SpamFighter, etc)
- Concepto de Firewalls - Ejercitación con productos de Firewalls Personales (Comodo, Checkpoint Zone Alarm, GFI VIPRE Firewall, etc)
- Concepto de Sistema de Prevención de Intrusos (IPS) - Ejercitación con productos de IPS personales (NIPS y HIPS) (Kaspersky Internet Security Suite, ESET Endpoint Protection, etc)
- Concepto de WEB Filtering o Control de URLs – Proxies y Proxies Reversos - Ejercitación con productos de WEB Filtering (WebTitan, K9, SafeSquid, etc)
- Concepto de Protección de Emails – Digital Rights Management - Ejercitación con productos de protección de Emails (Encryptics, PGP, etc)
- Protección para evitar Fuga de Información - Data Loss Prevention (DLP) - Ejercitación con productos de DLP (OpenDLP, DeviceLock, etc.) – Concepto de Llaves USB
- Concepto de Autenticación Fuerte (Strong Authentication) – Tokens – eTokens
- Concepto de Backups y Replicación de Datos
- Concepto de Inventario de HW y SW
- Protección de Dispositivos Mobile (Notebooks, netbooks, tablets, SmartPhones, etc)
- Procesamiento de LOGs y Correlación de Eventos – Ejercitación con productos de Event Log Analyzer

UNIDAD 3: Criptografía

- Conceptos de Criptografía – Criptoanálisis – Historia de la Criptografía clásica a la moderna
- Tipos de Criptografía: Simétrica, Asimétrica e Híbrida
- Métodos de cifrado – Algoritmos
- Métodos de Acceso Remoto Seguro
- Conceptos de RADIUS y TACACS
- Concepto de Firma Digital – Concepto de HASH – Integridad de Mensajes
- PKI - Conceptos de Clave Privada y Clave Pública
- Concepto de Certificados Digitales
- Relacionamiento entre Firma Digital y Certificados Digitales – Aplicaciones
- Criptografía Cuántica

UNIDAD 4: Forensia

- Concepto de Análisis Forense
- Análisis Forense de Seguridad Física
- Análisis Forense de Seguridad Informática
- Concepto de Evidencia Digital
- Metodología de Análisis forense
- Adquisición y Recolección de Evidencias

- Cadena de Guarda
- Exámen
- Análisis
- Reporte

UNIDAD 5: Arquitectura de Redes Seguras

- Arquitectura TCP/IP y el Modelo OSI
- Redes cableadas – Topologías – Medios físicos de redes
- Redes Wireless (Wi-Fi, Bluetooth, Access Point, Seguridad en Redes Wireless) - Concepto de WarDriving
- Concepto de Dispositivos UTM
- Concepto de Segmentación, Concepto de VLANs, Concepto de DMZ
- Conceptos de Seguridad en 1, 2 y 3 niveles
- Hacking Etico - Análisis de Vulnerabilidades y Penetration Tests – Auditoría de redes LAN - Ejercitación con productos de Análisis de Vulnerabilidades
- Conceptos de la ISO/IEC 27001 y 27002
- Autenticación – Access Control Lists (ACL) – OTP (One-Time-Password) – SSO (Single-Sign-On)

UNIDAD 6: Business Continuity Plan

- Concepto de Business Continuity Plan (BCP) y Concepto de Disaster Recovery Plan (DRP)
- Concepto de Análisis de Riesgos – Business Impact Analysis (BIA) – Recovery Tome Objective (RTO)
- Metodología de Diseño de un BCP – Fases
- Implementación de un BCP y un DRP
- Mantenimiento y Testing del BCP y DRP – Business Continuity Management (BCM)
- Tipos de Sitios de Contingencia
- Soluciones disponibles en los Servicios de Sitios de Contingencia – Storage on-demand – Archiving de Emails – Archiving de Imágenes de Video Vigilancia – Backups – Replicación de Datos – Vaulting de Medios Magnéticos
- Beneficios operativos y estratégicos del BCP – BCM

UNIDAD 7: Seguridad Física o Patrimonial

- Introducción a la Seguridad Física o Patrimonial
- Amenazas a la Seguridad Física
- Consideraciones en el Diseño de las Instalaciones – Cámaras – Video Vigilancia – Sensores - Alarmas
- Requerimientos de los Centros de Cómputos o Data Centers
- Controles de Acceso – Tipos – Tecnologías – Procesamiento de LOGs
- Controles de Seguridad Ambiental, Controles de Seguridad Industrial y Controles Administrativos
- Vigiladores – Rondines – Medios de Defensa no-letal – Films antivandalismo – Detectores de Metales

UNIDAD 8: Legislación

- Legislación en Argentina
- Ley de Delitos Informáticos
- Ley de Protección de Datos Personales
- Ley de Propiedad Intelectual y Derechos de Autor
- Regulaciones Nacionales e Internacionales

- BCRA A-4609
- PCI-DSS
- Sarbanes Oxley (SOX)
- HIPAA – ISO/IEC 27799
- Delitos contra Menores y Adolescentes en Internet – Seguridad en el Hogar

6. **BIBLIOGRAFÍA BÁSICA**

eBooks

a. Seguridad por Niveles, de Alejandro Corletti Estrada
b. El arte de la intrusión, Kevin Mitnick
c. La Etica de los Hackers, Pekka Himanen

7. **BIBLIOGRAFÍA DE CONSULTA**

Libros de formación Básica

a. Seguridad, Spam, Spyware y Virus, de Andy Walker
b. Firewall, de José Carballar
c. Manual Práctico de Seguridad de Redes, de Jan Harrington

Libros de Formación Avanzada

a. Seguridad de Redes, de Andrew Lockhart
b. Hackers 4, de Stuart McClure y otros
c. Edición Especial LINUX Máxima Seguridad, anónimo
d. La Biblia del Hacker, de Perez Agudin Justo y otros
e. Criptología y Seguridad de la Información, de Caballero Gil Pino y otro

8. **METODOLOGÍA DEL APRENDIZAJE**

8.a DESARROLLO DE LA ASIGNATURA

Inicialmente, se tratará de familiarizar al alumno, con los conceptos básicos, estadísticas, perfiles de ataques y potenciales atacantes, que se deben dominar para poder acceder al conocimiento de las técnicas de la seguridad de la información. Para el logro del objetivo indicado precedentemente, es necesario que el alumno adquiera conocimientos básicos en el área de las comunicaciones en general, redes y sus componentes, y la interacción de éstos con los servidores y puestos de trabajo existentes en las redes de las organizaciones.

No sólo se generará el conocimiento sobre seguridad de la información en formato electrónico, sino también en los aspectos físicos, completando los conocimientos con la seguridad ciudadana y de los individuos en el hogar.

Se proyectarán videos que permitan afianzar mejor los conecptos vertidos en las clases teóricas.

Finalmente se estudiaran diferentes tipos de soluciones, marcas de productos y estrategias de sus usos correspondientes, para que estén capacitados para la correcta elección de las soluciones a aplicar en seguridad.

8.b DINÁMICA DEL DICTADO DE LAS CLASES

Para favorecer estos logros, la metodología adoptada para el dictado de las clases es la siguiente se seguirán los siguientes lineamientos generales: El Profesor a cargo del curso se ocupará en forma personal y semanal del dictado de aquellos temas con un fuerte contenido teórico y que significan conceptos básicos y poco volátiles en la especialidad. Procederá a describir técnicas, características y pondrá ejemplos.

Éste generará un ámbito de reflexión y discusión de los temas presentados, para que mediante la intervención de los alumnos, se puedan aclarar aquellos aspectos que el docente puede captar a través de las consultas recibidas, como los que han resultado de más compleja compresión. También deberá discutir las distintas soluciones tecnológicas que se presentan un muchos casos, y mostrar ventajas y desventajas. Asimismo se complementará mediante sus clases semanales aquellos temas con Problemas de Aplicación de los temas teórico-conceptuales expuestos.

Se desarrollarán el Plan de Trabajos Prácticos acordados dentro de la cátedra, que incluirá siempre, dos áreas fundamentales: problemas y ejercicios de aplicación y trabajos prácticos de laboratorio.

En particular:

_ El profesor explicará en una primera fase los aspectos esenciales de cada tema, los días asignados para tales fines.

_ Los alumnos tendrán total libertad para interrumpir a los docentes, a los efectos de recabar aclaraciones, cuando las explicaciones no sean lo suficientemente claras.

_ Se usarán los equipos presentes en el gabinete de informática, para efectuar las prácticas técnicas o experimentales relativas a las acordadas con el profesor, y el empleo del equipamiento disponible.

Se buscará implementar trabajos prácticos a desarrollar con el auxilio de los docentes, según se detalla a continuación.

8.c TRABAJOS PRÁCTICOS

8.c.i ASPECTOS GENERALES.

Se efectuarán dos tipos diferentes de trabajos prácticos.

- Los primeros consistirán en la utilización de herramientas de seguridad, a fin de concoer su implementación, su comportamiento y su administración o gestión
- Los segundos, consistirán en la formulación de políticas, recomendaciones y diseño de segurización de redes.

8.c.ii ASPECTOS PARTICULARES.

Se desarrollarán problemas y ejercicios, con prácticas de laboratorio.

Problemas y ejercicios. La cátedra confeccionará una guía de trabajos prácticos que los alumnos deberán desarrollar. En ella estarán incluidos problemas y ejercicios. Los mismos deberán ser presentados para su aprobación como condición para la aprobación de los trabajos prácticos.

9. **METODOLOGÍA DE EVALUACIÓN**

9.a NORMAS DE EVALUACIÓN.

- El criterio es que la evaluación del alumno es permanente.
- Se tomarán dos exámenes parciales teórico/prácticos pudiendo acceder a un recuperatorio.
- Las notas de los parciales representan los resultados de la evaluación teórico/práctica.

- Los exámenes parciales y sus recuperatorios pueden ser orales o escritos.

9.b RÉGIMEN DE APROBACIÓN DE LA MATERIA.

- Para la aprobación de la materia los alumnos deberán tener los dos parciales aprobados, teniendo la posibilidad de recuperar cada UNO de ellos en dos oportunidades adicionales, en la fecha acordada con el profesor.
- Además los alumnos deberán aprobar los trabajos prácticos, como condición para la aprobación de la materia.
- Los alumnos que obtengan una nota inferior a cuatro puntos se les asignará la nota insuficiente y deberán recursar la materia.

10. **PLANIFICACIÓN**

CALENDARIO DE CLASES Y EVALUACIONES	
Semana 1	Unidad 1
Semana 2	Unidad 1
Semana 3	Unidad 2
Semana 4	Unidad 2 – Trabajo Práctico 1
Semana 5	Unidad 3
Semana 6	Unidad 3
Semana 7	Unidad 4 – Trabajo Práctico 2
Semana 8	Unidad 4 – Parcial 1
Semana 9	Unidad 5 – Recuperatorios
Semana 10	Unidad 5
Semana 11	Unidad 6 – Trabajo Práctico 3
Semana 12	Unidad 6
Semana 13	Unidad 7 – Trabajo Práctico 4
Semana 14	Unidad 7– Parcial 2
Semana 15	Unidad 8 - Recuperatorios
Semana 16	Unidad 8 – Repaso general
Del al de	FINAL

Información de Versiones	
Nombre del Documento:	Ficha Académica de la asignatura Seguridad Informática
Nombre del Archivo	Seguridad Informática – Plan 2008
Documento origen:	Seguridad Informatica – Plan 2013.doc
Elaborado por:	MBA Lic. Roberto Langdon
Revisado por:	Aníbal Romandetta
Aprobado por:	
Fecha de Elaboración:	3 de Abril de 2013
Fecha de Revisión:	12-4-2013
Fecha de aprobación	
Versión:	1.0