IDENTIFICACIÓN			
Nombre de la asignatura	**SEGURIDAD INFORMÁTICA**		
Código de la asignatura	SS804		
Programa Académico	Ingeniería de Sistemas		
Créditos académicos	3		
Trabajo semanal del estudiante	Docencia directa: 4	Trabajo Independiente: 5	
Trabajo semestral del estudiante	144		
Pre-requisitos	REDES Y COMUNICACIONES		
Co-requisitos			
Departamento oferente	Ingeniería de Sistemas		
Tipo de Asignatura	Teórico:	Teórico-Práctico: x	Práctico:
Naturaleza de la Asignatura	Habilitable:	No Habilitable: x	
	Validable:	No Validable:	
	Homologable: x	No Homologable:	

PRESENTACIÓN

El surgimiento de la sociedad de la información, y con ello el incremento en el uso de las Tecnologías de la Información y las Comunicaciones (TIC), hace que la información y los recursos informáticos que la gestionan tengan un rol principal en las actividades económicas, sociales y culturales. Asociado a este crecimiento es también cada vez mayor la cantidad de amenazas y ataques que se producen a las aplicaciones y recursos informáticos. Es en este contexto que la información se convierte en un recurso crítico al que hay que proteger. La seguridad informática se vuelve imprescindible como forma de garantizar la integridad, disponibilidad y confidencialidad de la información.

Las organizaciones deben estar preparadas para proteger sus activos de información. Esto implica conocer y aplicar de forma adecuada los conceptos, metodologías, herramientas, normativas y estándares existentes en esta materia, para lograr el objetivo de seguridad. Para ello se requiere de recursos humanos profesionales debidamente capacitados y actualizados, que puedan aplicar de forma exitosa las metodologías y adaptarse rápidamente a los cambios tecnológicos y las exigencias de un área que está en constante evolución y cambio.

JUSTIFICACIÓN

Un profesional de la ingeniería de sistemas debe tener conocimientos en seguridad informática, debe ser capaz de aplicar las metodologías, tecnologías y herramientas que existen en las distintas áreas involucradas, como ser criptografía, modelos formales, análisis forense, etc., así como en las áreas en las que la seguridad informática tiene su aplicación: redes, sistemas operativos, aplicaciones. Deben también ser capaces de gestionar la seguridad de la información, aplicando las normativas y estándares existentes, gestionando

los incidentes, los riesgos y garantizar la continuidad del negocio, protegiendo los activos críticos.
En la actualidad, e impulsada por el surgimiento de estándares, leyes y normativas, la seguridad se convierte en un requisito fundamental para cualquier tipo de organización. No sólo es un requerimiento de los bancos u organizaciones financieras, sino que se extiende a todo tipo y tamaño de organización. Los riesgos de ataques informáticos alcanzan a todas las organizaciones por igual, impactando directamente en su negocio. Los profesionales informáticos deben estar preparados para poder gestionar, enfrentar y mitigar estos riesgos.
Este escenario lleva a la necesidad de ofrecer formación académica, de forma de preparar recursos humanos de alto nivel para enfrentar los nuevos retos asociados a la Seguridad Informática. Brindar unos conocimientos en el área que permita a los estudiantes incorporar un sólido marco teórico y a través del uso de laboratorios y trabajos prácticos, adquirir la práctica necesaria para enfrentar los nuevos retos que presentan las vulnerabilidades y amenazas.

OBJETIVO GENERAL

Adquiera los conocimientos básicos sobre los aspectos fundamentales de la seguridad informática e implementar medidas de seguridad en un sistema informático.
Formar profesionales éticos capaces de implementar las mejores prácticas y tendencias, conocer y cumplir las normativas y regulaciones nacionales e internacionales, generar y transmitir conocimiento en el área de forma de alcanzar mayores y mejores niveles de seguridad de la información.

OBJETIVOS ESPECÍFICOS

- Introducir los conceptos básicos de seguridad informática.
- Diseñar y/o implantar mecanismos de seguridad, con el objetivo de desarrollar, ampliar o mejorar las plataformas de computación.
- Adquirir los conceptos básicos necesarios para identificar las posibles amenazas que puede sufrir un sistema informático y establecer los mecanismos de protección adecuados que garanticen la seguridad del mismo. Incluye, pero no está limitado a la seguridad informática en los sistemas operativos y redes de datos TCP/IP.
- Introducir conceptos asociados a la seguridad en el proceso de desarrollo de aplicaciones.
- Comprender qué hitos tener en cuenta a la hora de construir aplicaciones seguras en el proceso de desarrollo, y entender los errores más comunes que se presentan en la codificación de las aplicaciones.
- Introducir a los estudiantes en los principales conceptos y metodologías asociadas a la gestión de seguridad de la información, en el marco normativo internacional y nacional existente.
- Llevar a la práctica una metodología de rápida aplicación para la implementación de un Sistema de Gestión de Seguridad de la Información.

- Presentar metodologías concretas para la gestión de riesgos y gestión de
- incidentes. Se abarcarán los principales conceptos en torno a la familia de normas ISO/IEC 27000.
- Introducción a los fundamentos principales de criptografía y su aplicación en los mecanismos de protección contra amenazas de seguridad, integrando aspectos teóricos con laboratorios experimentales.

COMPETENCIAS GENERALES Y ESPECÍFICAS

Se espera que el estudiante al terminar el curso tenga la capacidad para:

- Dominar las áreas fundamentales de la Seguridad Informática.
- Ser capaz de tomar decisiones éticas y practicar un comportamiento ético profesional.
- Implementar un plan estratégico para gestionar la seguridad de la información en cualquier organización.
- Gestionar los riesgos y el impacto que los mismos puedan tener en el negocio de la organización.
- Conocer y aplicar las mejores prácticas, tendencias y herramientas para mitigar los riesgos asociados a las diferentes tecnologías de la información
- Implementar metodologías adecuadas para garantizar la continuidad del negocio de la organización.
- Aprender nuevos modelos, técnicas y tecnologías cuando estas emergen, y apreciar la necesidad de ese desarrollo profesional continuo.
- Diagnosticar la situación de una organización y brindar asesoramiento en materia de seguridad informática.
- Gestionar los incidentes de forma efectiva y profesional.

METODOLOGÍA

Esta asignatura, cuya organización está diseñada en unidades temáticas, que se desarrollarán en forma secuencial está diseñada para que el estudiante lo realice en el transcurso del semestre académico. Cada una de las unidades presenta su propósito, objetivos de aprendizaje, contenidos, metodología, criterios de evaluación e incluye documentos de lectura, trabajos grupales e individuales, algunos de ellos el estudiante los desarrollará en la hora de clase y otros fuera del horario normal de la asignatura, los cuales deberán entregar al docente ya sea en formato digital o impresos. Durante el semestre se desarrollará el proyecto de aula el cual debe hacer entregas parciales al finalizar cada corte. Se preparará pruebas objetivas con los lineamientos que serán debidamente señalados y se solicitará algunas actividades tales como mapas conceptuales, ensayos o resúmenes.

ESTRATEGIAS METODOLÓGICAS

Para dar aplicabilidad a la estructura curricular se establecen las siguientes estrategias metodológicas en concordancia con lo establecido en el modelo pedagógico Upecista y contenidas en las actividades académicas:

Trabajo presencial o acompañamiento directo: consiste en el tiempo dedicado a la actividad académica en la que hay interacción entre el docente y el estudiante, a través de clases magistrales, seminarios, talleres, y laboratorios; donde se da explicación a los temas programados en el curso, se realiza en las instalaciones de la institución en horarios definidos previamente y en espacios destinados para ello tales como: salones de clases, salas de sistemas e informática, laboratorios, visitas técnicas y demás lugares que permitan y cumplan con las normas exigidas para impartir clases.

Trabajo independiente: consiste en el tiempo asumido por el estudiante y que dedica al aprendizaje autónomo, cuyas actividades pueden ser consultas, lecturas, trabajos en grupo entre otros, las cuales puede realizarlas en sitios comunes tales como biblioteca, aulas abiertas, laboratorios, salas de sistemas e informáticas, campus virtual, herramientas sincrónicas y asincrónicas(wikis, correo electrónico, sites, redes sociales) en horarios diferentes a los establecidos para el desarrollo de las actividades académicas programadas.

Asesorías: se enfoca en las actividades, prácticas formativas, trabajos de campo que el estudiante realiza y que requiere una orientación directa del docente, donde se tratan temas de interés concernientes a la asignatura y solución a inquietudes; estas son programadas por el docente en horarios diferentes a los establecidos para el desarrollo académico de los cursos.

Talleres. Esta estrategia metodológica fortalece el proceso de enseñanza- aprendizaje; el taller es una actividad práctica que promueve un espacio de reflexión y construcción del conocimiento; estos son previamente diseñados por los docentes con base a las competencias que el estudiante debe desarrollar en cada asignatura y publicados en espacios tales como: sites, blogs, aula web o aula de clases. Las asignaturas de tipo teórico - práctico usan esta estrategia para promover el trabajo en equipo, consultas y profundización investigativa.

Mediaciones Virtuales. El uso y apropiación de las tics se convierten en herramientas claves que son de apoyo al proceso de formación en el aula de clases, debido a que promueven en el estudiante la búsqueda permanente del conocimiento a través de herramientas como: plataformas virtuales- aula web, redes profesionales, sociales, sites, aplicaciones en la nube, correo electrónico, foros y demás herramientas sincrónicas y asincrónicas que facilitan la interacción.

Prácticas formativas: se definen como el proceso mediante el cual el estudiante del programa de Ingeniería de sistemas, realiza actividades y procedimientos que le permitan la aplicación de sus conocimientos y habilidades en un escenario laboral en tiempo real y en espacios pedagógicos de cooperación mutua que faciliten la identificación de problemas en las empresas en coherencia con su disciplina profesional. En este sentido, la práctica formativa se constituye en una opción de grado para el estudiante, evidenciado en la formulación y ejecución de un proyecto aplicado que brinde soluciones de ingeniería y permita la optimización de los procesos en el contexto empresarial seleccionado por el mismo, lo cual será validado mediante el cumplimiento de los objetivos formulados.

Laboratorios: fomenta la puesta en marcha de los conceptos teóricos adquiridos en clase y que pueden ser reforzados a través de la práctica, direccionadas por el docente a través de guías especificas donde se ilustran las actividades y los objetivos de la práctica. Es importante indicar que en el programa de ingeniería de sistemas asignaturas como (física, mecánica, arquitectura de computadores, redes de computadores entre otras) requieren de estos espacios para el proceso de formación académica.

Horas de Asesoría: Esta estrategia corresponde a la asesoría que debe brindar el docente a los estudiantes, sobre las tareas asignadas y en horas estipuladas independientemente de las horas de docencia directa.

Proyecto de aula: Tiene como finalidad que los estudiantes durante el desarrollo del curso y organizado por fases organicen el proyecto de aula con base a las temáticas abordadas y dando solución a una necesidad del entorno.

CONTENIDO

CAPÍTULO 1. PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA
1.1 QUÉ SE ENTIENDE POR SEGURIDAD INFORMÁTICA
1.2 OBJETIVOS DE LA SEGURIDAD INFORMÁTICA
1.3 SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN
1.4 CONSECUENCIAS DE LA FALTA DE SEGURIDAD
1.5 PRINCIPIO DE “DEFENSA EN PROFUNDIDAD”
1.6 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
1.6.1 Implantación de un Sistema de Gestión de Seguridad de la Información
1.7 ANÁLISIS Y GESTIÓN DE RIESGOS EN UN SISTEMA INFORMÁTICO
1.7.1 Recursos del sistema
1.7.2 Amenazas
1.7.3 Vulnerabilidades
1.7.4 Incidentes de Seguridad
1.7.5 Impactos
1.7.6 Riesgos

1.7.7 Defensas, salvaguardas o medidas de seguridad
1.7.8 Transferencia del riesgo a terceros

CAPÍTULO 2. POLÍTICAS, PLANES Y PROCEDIMIENTOS DE SEGURIDAD
2.1 INTRODUCCIÓN Y CONCEPTOS BÁSICOS
2.2 DEFINICIÓN E IMPLANTACIÓN DE LAS POLÍTICAS DE SEGURIDAD
2.3 INVENTARIO DE LOS RECURSOS Y DEFINICIÓN DE LOS SERVICIOS OFRECIDOS
2.4 SEGURIDAD FRENTE AL PERSONAL
2.4.1 Alta de empleados
2.4.2 Baja de empleados
2.4.3 Funciones, obligaciones y derechos de los usuarios
2.4.4 Formación y sensibilización de los usuarios
2.5 ADQUISICIÓN DE PRODUCTOS
2.6 RELACIÓN CON PROVEEDORES
2.7 SEGURIDAD FÍSICA DE LAS INSTALACIONES
2.8 SISTEMAS DE PROTECCIÓN ELÉCTRICA
2.9 CONTROL DEL NIVEL DE EMISIONES ELECTROMAGNÉTICAS
2.10 VIGILANCIA DE LA RED Y DE LOS ELEMENTOS DE CONECTIVIDAD
2.11 PROTECCIÓN EN EL ACCESO Y CONFIGURACIÓN DE LOS SERVIDORES
2.12 SEGURIDAD EN LOS DISPOSITIVOS DE ALMACENAMIENTO
2.13 PROTECCIÓN DE LOS EQUIPOS Y ESTACIONES DE TRABAJO
2.14 CONTROL DE LOS EQUIPOS QUE PUEDEN SALIR DE LA ORGANIZACIÓN
2.15 COPIAS DE SEGURIDAD
2.16 GESTIÓN DE SOPORTES INFORMÁTICOS
2.17 GESTIÓN DE CUENTAS DE USUARIOS
2.18 IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS
2.19 AUTORIZACIÓN Y CONTROL DE ACCESO LÓGICO
2.20 MONITORIZACIÓN DE SERVIDORES Y DISPOSITIVOS DE LA RED
2.21 PROTECCIÓN DE DATOS Y DE DOCUMENTOS SENSIBLES
2.22 SEGURIDAD EN LAS CONEXIONES REMOTAS
2.23 DETECCIÓN Y RESPUESTA ANTE INCIDENTES DE SEGURIDAD
2.24 OTROS ASPECTOS A CONSIDERAR
2.24.1 Seguridad en el desarrollo, implantación y mantenimiento de aplicaciones informáticas
2.24.2 Seguridad en las operaciones de administración y mantenimiento de la red y de los equipos
2.24.3 Creación, manejo y almacenamiento de documentos relacionados con la seguridad del sistema informático
2.24.4 Cumplimiento de la legislación vigente
2.24.5 Actualización y revisión de las medidas de seguridad
2.25 REALIZACIÓN DE PRUEBAS Y AUDITORÍAS PERIÓDICAS

CAPÍTULO 3. LA IMPORTANCIA DEL FACTOR HUMANO EN LA SEGURIDAD
3.1 EL FACTOR HUMANO EN LA SEGURIDAD INFORMÁTICA
3.2 FUNCIONES Y RESPONSABILIDADES DE LOS EMPLEADOS Y DIRECTIVOS
3.3 INGENIERÍA SOCIAL
3.4 FORMACIÓN DE LOS USUARIOS
3.5 EL CONTROL Y SUPERVISIÓN DE LOS EMPLEADOS

3.5.1 El uso de los servicios de Internet en el trabajo
3.5.2 Herramientas para el control y vigilancia del acceso a los servicios de Internet

CAPÍTULO 4. ESTANDARIZACIÓN Y CERTIFICACIÓN EN SEGURIDAD INFORMÁTICA
4.1 ESTÁNDARES DE SEGURIDAD
4.1.1 Propósito de los estándares
4.1.2 Organismos responsables de la estandarización
4.2 ESTÁNDARES ESTADOUNIDENSES
4.2.1 TCSEC: Trusted Computer System Evaluation Criteria
4.2.2 Federal Criteria
4.2.3 FISCAM: Federal Information Systems Controls Audit Manual
4.2.4 NIST SP 800
4.3 ESTÁNDARES EUROPEOS
4.3.1 ITSEC: Information Technology Security Evaluation Criteria
4.3.2 ITSEM: Information Technology Security Evaluation Metodology
4.3.3 Agencia Europea de Seguridad de la Información y las Redes
4.4 ESTÁNDARES INTERNACIONALES
4.4.1 ISO/IEC 15408: Common Criteria
4.4.2 ISO/IEC 17799
4.4.3 BS 7799 Parte 2:2002
4.4.4 Familia ISO/IEC 27000
4.4.4.1 ISO/IEC 27000
4.4.4.2 ISO/IEC 27001
4.4.4.3 ISO/IEC 27002
4.4.4.4 ISO/IEC 27003
4.4.4.5 ISO/IEC 27004
4.4.4.6 ISO/IEC 27005
4.4.4.7 ISO/IEC 27006
4.4.5 Estándares relacionados con los sistemas y servicios criptográficos
4.6 PROCESO DE CERTIFICACIÓN

CAPÍTULO 5. VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS
5.1 INCIDENTES DE SEGURIDAD EN LAS REDES
5.2 CAUSAS DE LAS VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS
5.2.1 Debilidad en el diseño de los protocolos utilizados en las redes
5.2.2 Errores de programación
5.2.3 Configuración inadecuada de los sistemas informáticos
5.2.4 Políticas de Seguridad deficientes o inexistentes
5.2.5 Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática
5.2.6 Disponibilidad de herramientas que facilitan los ataques
5.2.7 Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías
5.2.8 Existencia de “puertas traseras” en los sistemas informáticos
5.2.9 Descuido de los fabricantes
5.3 TIPOS DE VULNERABILIDADES
5.3.1 Vulnerabilidades que afectan a equipos

5.3.1.1 ROUTERS Y CABLE-MÓDEMS
5.3.1.2 CÁMARAS WEB Y SERVIDORES DE VÍDEO
5.3.1.3 VULNERABILIDADES EN OTROS EQUIPOS CONECTADOS A UNA RED: IMPRESORAS, ESCÁNERES, FAXES...
5.3.1.4 TELÉFONOS MÓVILES
5.3.2 Vulnerabilidades que afectan a programas y aplicaciones informáticas
5.3.2.1 SISTEMAS OPERATIVOS, SERVIDORES Y BASES DE DATOS
5.3.2.2 NAVEGADORES
5.3.2.3 APLICACIONES OFIMÁTICAS COMO WORD O EXCEL
5.3.2.4 OTRAS UTILIDADES Y APLICACIONES INFORMÁTICAS
5.4 RESPONSABILIDADES DE LOS FABRICANTES DE SOFTWARE
5.5 HERRAMIENTAS PARA LA EVALUACIÓN DE VULNERABILIDADES
5.5.1 Análisis y evaluación de vulnerabilidades
5.5.2 Ejecución de Tests de Penetración en el Sistema
5.6 Análisis Forense
5.6.1 Recopilación de evidencias
5.6.2 Análisis e investigación de evidencias
5.6.3 Documentación del análisis
5.6.4 Herramientas informáticas de apoyo al análisis forense

CAPÍTULO 6. AMENAZAS A LA SEGURIDAD INFORMÁTICA
6.1 CLASIFICACIÓN DE LOS INTRUSOS EN LAS REDES
6.1.1 Hackers
6.1.2 Crackers (“blackhats”)
6.1.3 Sniffers
6.1.4 Phreakers
6.1.5 Spammers
6.1.6 Piratas informáticos
6.1.7 Creadores de virus y programas dañinos
6.1.8 Lamers (“wannabes”): “Script-kiddies” o “Click-kiddies”
6.1.9 Amenazas del personal interno
6.1.10 Ex-empleados
6.1.11 Intrusos remunerados
6.1.12 Algunos “hackers”, “crackers” y “phreakers” famosos
6.1.12.1 JOHN DRAPER, “CAPITÁN CRUNCH”
6.1.12.2 VLADIMIR LEVIN
6.1.12.3 KEVIN POULSON

EVALUACIÓN

	TIPO DE EVALUACIÓN	FECHA	PORCENTAJE
	Parcial escrito, Laboratorios de casos de	Las fechas	30%

PRIMER CORTE	estudio en grupo, Pruebas orales/escritas rápidas (Quizes), Revisión y entrega Primera fase de proyecto.	estarán acorde a las programadas por el calendario académico para el periodo en Curso.	
SEGUNDO CORTE	Parcial escrito, laboratorios de casos de estudio en grupo, Pruebas orales/escritas rápidas (Quizes), Lecturas y temas de investigación sustentadas, revisión y entrega segunda fase de proyecto.		30%
PROYECTO FINAL	Entrega de proyecto final con todas las fases del trabajo y sustentación, que evalúe las competencias exigidas.		40%

REFERENCIAS BIBLIOGRÁFICAS

- Costas Santos, Jesús. Seguridad Informática. Ra-Ma. Ediciones de la U, Bogotá 2011.
- Gomez Vieites, Alvaro. Auditoria de seguridad informática. Ediciones de la U, Bogotá 2013
- CANO, Jeimy J. Pautas y Recomendaciones para Elaborar Políticas de Seguridad Informática (PSI). Bogotá. 2001.
- RODRIGUEZ, Luis Ángel. Seguridad de la Información en Sistemas de Cómputo. Ventura Ediciones, México, 1995.

FUNDAMENTOS DE SEGURIDAD EN REDES,
STALLINGS,
2003

DISEÑO DE SEGURIDAD EN REDES PEARSON EDUCACION Autor: FRAGUAS BERASAIN, SANTIAGO 2003.

*Seguridad en WiFi / Stewart S. Miller ; traducción y revisión técnica Rafael Rodríguez de Cora, Gregorio Pérez Van Kappel. MCGRAW-HILL INTERAMERICANA Autor: PÉREZ VAN KAPPEL, GREGORIO.TR 2004.

SEGURIDAD EN REDES TELEMATICAS MCGRAW HILL INTERAMERICANA DE ESPAÑA Autor: CARRACEDO GALLARDO JUSTO 2004.

FIREWALLS: MANUAL DE REFERENCIA MCGRAW HILL INTERAMERICANA Autor: ANTONIO TOCA CASO. TR 2003.
Claves Hackers en Linux y Unix / Nitesh Dhanjani,Tr. Gregorio Caraballo Montaño MCGRAW-HILL INTERAMERICANA DE ESPAÑA Autor: CARABALLO MONTAÑO GREGORIO, TR. 2004.

*Seguridad informática: básico EDICIOENS ECOE Autor: GÓMEZ VIEITES, ÁLVARO 2011.

*Superutilidades Hackers / Keith J. Jones, Mike Shema, Bradley C. Johnson ; traducción Jorge Rodríguez Vega. MCGRAW HILL INTERMARICANA Autor: RODRÍGUEZ VEGA, JORGE...TR. 2003.

Claves Hackers en Windows / Michael O Dea, Tr. Jorge Rodríguez Vega MCGRAW-HILL INTERAMERICANA DE ESPAÑA Autor: RODRÍGUE VEGA JORGE, TR. 2004.

Avances en Criptología y Seguridad de la Información / Directores: Benjamín Ramos Álvarez...(et. al.). EDICIONES DÍAZ DE SANTOS Autor: RAMOS ÁLVAREZ, BENJAMÍN...(ET. AL.) 2004.

INTRODUCCION A LA CRIPTOGRAFIA ALFA OMEGA Autor: CABALLERO GIL PIND 2003.

*Técnicas criptográficas de protección de datos / Amparo Fúster Sabater... [et al.]. EDITOR ALFAOMEGA Autor: MUÑOS MASQUÉ, JAIME...COAUT. 1998.