2016B

ACADEMIA DE ARQUITECTURA DE COMPUTADORAS							
I	**NOMBRE DE LA MATERIA**	**SEGURIDAD**					
	TIPO DE ASIGNATURA	CURSO			**CLAVE**	I7037	
II	**CARRERA**	LICENCIATURA EN INGENIERIA EN COMPUTACION LICENCIATURA EN ING. EN TELEMATICA LIC. EN ING. EN COMUNICACIÓN MULTIMEDIA					
	ÁREA DE FORMACIÓN	BÁSICA COMÚN					
III	**PRERREQUISITOS**	NINGUNO					
IV	**CARGA GLOBAL TOTAL**	68	**TEORÍA**	57	**PRÁCTICA**	17	
V	**VALOR EN CRÉDITOS**	8					
FECHA DE CREACIÓN	Julio 2015 (2015B)	**FECHA DE MODIFICACIÓN**	- - -		**FECHA DE EVALUACIÓN**	Julio 2016 (2016B)	

VI. OBJETIVOS

OBJETIVO GENERAL:
El alumno comprenderá y aplicará los métodos y elementos que le permitan planificar el desarrollo de un entorno de seguridad, con base en la identificación y análisis de amenazas, ataques y vulnerabilidades en los sistemas y redes de cómputo, enmarcados en una base ética

OBJETIVOS PARTICULARES:

1. Fundamentos teóricos

Objetivo: El alumno conocerá los conceptos, objetivos y antecedentes históricos de la Seguridad informática, así como el de los modelos de seguridad que le permitan adoptar los Estándares destinados a planificar un esquema de seguridad en una organización.

2. Amenazas y vulnerabilidades

Objetivo: El alumno conocerá, identificará y explicará los diferentes tipos de amenazas y vulnerabilidades así como las fuentes que las ocasionan.

3. Identificación de ataques y técnicas de intrusión

Objetivo: El alumno conocerá, identificará y explicará los métodos y técnicas de ataque e intrusión a redes y sistemas; a su vez conocerá los mecanismos y herramientas para evitarlos.

4. Políticas de seguridad informática de la organización

Objetivo: El alumno entenderá, explicará, valorará y adquirirá la capacidad para desarrollar políticas de seguridad informática así como los procedimientos y planes de contingencia que le permitan mantener el control de la seguridad en una organización.

5 Análisis del riesgo

Objetivo: El alumno conocerá, identificará, seleccionará y aplicará las técnicas y métodos que le permitan llevar a cabo actividades concernientes a la evaluación de riesgos dentro de una organización.

6. Ética informática

Objetivo: El alumno comprenderá y conocerá la importancia de enmarcar la Seguridad Informática en un ambiente ético y profesional.

VII. CONTENIDO TEMÁTICO

1. Fundamentos teóricos

Objetivo: El alumno conocerá los conceptos, objetivos y antecedentes históricos de la Seguridad informática, así como el de los modelos de seguridad que le permitan adoptar los Estándares destinados a planificar un esquema de seguridad en una organización.

Contenido:

1.1 Introducción
1.1.1 Concepto de la Seguridad Informática
1.1.2 Evolución histórica de la Seguridad Informática
1.1.3 Objetivos y misión de la Seguridad Informática
1.1.4 Amenazas a las redes y sistemas computacionales
1.2 Normatividad de la Seguridad Informática
1.2.1 Normas de Seguridad a través de la Historia
1.2.1.1 TCSEC / Libro Naranja
1.2.1.2 ITSEC
1.2.1.3 CTCPEC
1.2.1.4 FC-ITS
1.2.2 Criterios Comunes / ISO 15408
1.2.3 ISO 17799
1.2.4 Nuevas Tendencias
1.2.4.1 OCTAVE
1.3 Esquema de Seguridad basado en Criterios Comunes: Perfiles de Protección
1.3.1 Definición y propósito
1.3.2 Estructura
1.3.2.1 Introducción
1.3.2.2 Descripción del objeto de evaluación
1.3.2.3 Entorno de seguridad
1.3.2.4 Hipótesis
1.3.2.5 Amenazas
1.3.2.6 Políticas de la organización
1.3.2.7 Nivel de Garantía general requerido
1.3.2.8 Objetivos de Seguridad
1.3.2.9 Requerimientos Funcionales y de Garantía
1.3.2.10 Justificación
1.4 Servicios de Seguridad
1.4.1 Confidencialidad
1.4.2 Autenticación
1.4.3 Integridad
1.4.4 No repudio
1.4.5 Control de Acceso
1.4.6 Disponibilidad

2. Amenazas y vulnerabilidades

Objetivo: El alumno conocerá, identificará y explicará los diferentes tipos de amenazas y vulnerabilidades así como las fuentes que las ocasionan.

Contenido:

2.1 Amenazas
2.1.1 Definición

2.1.2 Fuentes de amenaza
2.1.2.1 Factor humano
2.1.2.1.1 Tipos: ingeniería social, robo, fraude, sabotaje, personal enterado, terroristas, curiosos, intrusos remunerados, etc.
2.1.2.1.2 Hardware
2.1.2.1.3 Tipos: mal diseño, errores de fabricación, suministro de energía, etc.
2.1.2.2 Red de datos
2.1.2.2.1 Tipos: topología seleccionada, sistema operativo, sistema de administración, monitoreo, etc.
2.1.2.3 Software
2.1.2.3.1 Tipos: software de desarrollo, software de aplicación, código malicioso, virus, etc.
2.1.2.4 Desastres naturales
2.1.2.4.1 Tipos: inundaciones, terremotos, fuego, viento, tormentas eléctricas, etc.

2.2 Vulnerabilidades
2.2.1 Definición
2.2.2 Tipos de Vulnerabilidades
2.2.2.1 Física
2.2.2.2 Natural
2.2.2.3 Hardware
2.2.2.4 Software
2.2.2.5 Red

3. Identificación de ataques y técnicas de intrusión

Objetivo: El alumno conocerá, identificará y explicará los métodos y técnicas de ataque e intrusión a redes y sistemas; a su vez conocerá los mecanismos y herramientas para evitarlos.

Contenido:

3.1 Reconocimiento y Obtención de Información
3.1.1 Bases de Datos Públicas
3.1.2 WEB
3.1.3 DNS
3.1.4 Keyloggers
3.1.5 Ingeniería Social
3.1.6 Otros

3.2 Identificación de Vulnerabilidades
3.2.1 Ataques a Redes Telefónicas
3.2.2 Ataques a la Telefonía Inalámbrica
3.2.3 Barrido de Puertos
3.2.4 Identificación de Firewalls
3.2.4.1 Interpretación de reglas y filtros
3.2.5 Identificación de Sistemas Operativos / Fingerprinting
3.2.5.1 Métodos de Identificación
3.2.6 Escaneo a Redes Inalámbricas
3.2.7 Instalaciones Físicas
3.2.8 Configuración de Servicios y Servidores
3.2.9 Software
3.2.10 Otros

3.3 Explotación y obtención de acceso a Sistemas y Redes
3.3.1 Promiscuidad en Redes
3.3.2 Robo de Identidad

3.3.3 Engaño a Firewalls y Detectores de Intrusos
3.3.4 Vulnerabilidades en el Software
3.3.4.1 Buffer Overflows
3.3.4.2 Heap Overflows
3.3.4.3 Formato de Cadena
3.3.4.4 Race Conditions
3.3.4.5 SQL Injection
3.3.4.6 Cross-Site & Cross-Domain Scripting
3.3.4.7 Virus y Gusanos
3.3.4.8 Otros
3.3.5 Ataques a Contraseñas
3.3.6 Debilidad de los Protocolos de Red
3.3.7 Ataques a Servicios
3.3.8 Negación de Servicio
3.3.9 Ataques a Redes Inalámbricas
3.3.9.1 Denegación de Servicio
3.3.9.2 Ataque de Hombre en Medio
3.3.9.3 ARP Poisoning
3.3.9.4 WEP key-cracking
3.3.9.5 Nuevos Métodos de Ataque en Redes Inalámbricas
3.4 Mantener el Acceso a Sistemas Comprometidos
3.4.1 Puertas Traseras
3.4.2 Caballos de Troya
3.4.3 Rootkits
3.4.4 Otros
3.5 Eliminación de Evidencias
3.5.1 Edición de bitácoras
3.5.2 Ocultar Información
3.5.3 Estenografía
3.5.4 Nuevos métodos

4. Políticas de seguridad informática de la organización

Objetivo: El alumno entenderá, explicará, valorará y adquirirá la capacidad para desarrollar políticas de seguridad informática así como los procedimientos y planes de contingencia que le permitan mantener el control de la seguridad en una organización.

Contenido:

4.1 Políticas de Seguridad Informática
4.1.1 Objetivo de una política de seguridad
4.1.2 Misión, visión y objetivos de la organización
4.1.3 Principios fundamentales de las políticas de seguridad
4.1.3.1 Responsabilidad individual
4.1.3.2 Autorización
4.1.3.3 Mínimo privilegio
4.1.3.4 Separación de obligaciones
4.1.3.5 Auditoría
4.1.3.6 Redundancia
4.1.4 Políticas para la confidencialidad
4.1.5 Políticas para la integridad
4.1.6 Modelos de Seguridad: abstracto, concreto, de control de acceso y de flujo de información

4.1.7 Desarrollo de políticas orientadas a servicios de seguridad
4.1.8 Publicación y Difusión de las Políticas de Seguridad
4.2 Procedimientos y Planes de Contingencia
4.2.1 Procedimientos Preventivos
4.2.2 Procedimientos Correctivos
4.2.3 Planes de Contingencia
4.2.3.1 Objetivos y Características de un Plan de Contingencias
4.2.3.2 Fases del Plan de Contingencia
4.2.3.2.1 Análisis y Diseño
4.2.3.2.2 Desarrollo de un plan de contingencias
4.2.3.2.3 Pruebas y Mantenimiento

5 Análisis del riesgo

Objetivo: El alumno conocerá, identificará, seleccionará y aplicará las técnicas y métodos que le permitan llevar a cabo actividades concernientes a la evaluación de riesgos dentro de una organización.

Contenido:

5.1 Terminología básica
5.1.1 Activos
5.1.2 Riesgo
5.1.3 Aceptación
5.1.4 Análisis del riesgo
5.1.5 Manejo del riesgo
5.1.6 Evaluación
5.1.7 Impacto
5.1.8 Pérdida esperada
5.4.4 Impacto de la ocurrencia de una amenaza
5.4.5 Controles en el lugar
5.4.6 Riesgos residuales
5.4.7 Identificación de los controles adicionales
5.4.8 Preparación de un informe del análisis del riesgo.
5.1.9 Vulnerabilidad
5.1.10 Amenaza
5.1.11 Riesgo residual
5.1.12 Controles
5.2 Análisis cuantitativo
5.3 Análisis cualitativo
5.4 Pasos del análisis de riesgo
5.4.1 Identificación y evaluación de los activos
5.4.2 Identificación de amenazas
5.4.3 Identificación de vulnerabilidades
5.5 Análisis costo-beneficio

6. Ética informática

Objetivo: El alumno comprenderá y conocerá la importancia de enmarcar la Seguridad Informática en un ambiente ético y profesional.

Contenido:

6.1 Concepto de Ética Informática
6.2 Códigos Deontológico en Informática

6.3 Contenidos de la Ética Informática
6.4 Actualidad de la Ética Informática
6.5 Psicología del Intruso
6.6 Códigos de Ética
6.7 Casos de Estudio

VIII. MODALIDAD DEL PROCESO DE ENSEÑANZA-APRENDIZAJE

Las modalidades propuestas para la impartición de este curso son 2:

1. ***Presencial: 100% presencial***

Las actividades de enseñanza y aprendizaje se llevan a cabo en un aula o laboratorio.

2. ***Mixta: 30% en línea y 70% presencial***

Las actividades y recursos se llevan a cabo en la plataforma: moodle.cuc.udg.mx

IX. BIBLIOGRAFÍA

BIBLIOGRAFIA BASICA

- ANONYMOUS, *Maximun Security,* 4rd. Edition, U.S.A.
- Sams Publishing, 2003, FACCIN, Stefano, et al., *IP in Wireless Networks,* U.S.A., Prentice Hall, 2003.
- FLICKENGER, Rob, *Linux Server Hacks,* U.S.A., O'Reilly, 2003.
- GARFINKEL, Simson, SCHWARTZ, Alan, SPAFFORD, Gene., *Practical UNIX & Internet Security,* 3rd. Edition, U.S.A.
- O'Reilly, 2003, KING, Todd, *Security + Training Guide,* U.S.A., Que, 2003.

BIBLIOGRAFIA COMPLEMENTARIA

- LOPEZ, Jaquelina y QUEZADA, Cintia, *Apuntes de Seguridad Informática,* México, Facultad de Ingeniería – UNAM, 2005
- McCARHY, Linda, *IT security: risking the corporation,* U.S.A., Prentice Hall, 2003.

XVI. CONOCIMIENTOS, APTITUDES, ACTITUDES, VALORES, CAPACIDADES Y HABILIDADES QUE EL ALUMNO DEBE ADQUIRIR

Aptitud: Capacidad y disposición para el buen manejo de actividades de informática y habilidad para ejercer ciertas tareas minimizando tiempo y esfuerzo, logrando con esto las condiciones idóneas para realizar actividades dependiendo el área laboral.
Actitud: Se pretende que el alumno, cuente con una conducta positiva hacia el manejo de estas herramientas necesarias, para la seguridad de la información usando las tecnologías en la actualidad.
Valores: Se pretende que el alumno al finalizar el curso, le permita manifestar su identidad en relación a sus nuevos conocimientos tanto en su trayecto escolar con su delación con el exterior.
Conocimiento: Este curso tiene como objetivo principal el llevar a cabo un proceso de retroalimentación para adquirir los conocimientos necesarios a través de dinámicas de evaluación para reafirmar y estimular al alumno.
Capacidades: El alumno tendrá la capacidad de prevenir perdida de información, así como también mejorar los procesos en tiempo y forma para realizarlo dependiendo de las circunstancias en que se presente.
Habilidades: El alumno tendrá la disposición para realizar tareas relacionadas con el área de seguridad, basándose en una adecuada percepción de los estímulos externos y una respuesta activa que redunde en una actuación eficaz, es decir, contara con el potencial para adquirir y manejar nuevos conocimientos y destrezas.

Valores Éticos y Sociales: El estudiante debe trabajar individualmente (Responsabilidad y puntualidad); Valorar objetivamente el trabajo y opiniones de sus compañeros (Respeto); Resolver exámenes individualmente (Honestidad); Valorar el método de la ciencia como un camino que nos conduce a la verdad (Valorar la verdad); Auto motivarse para administrar su propio tiempo y cumplir con las tareas que se le asignen en el curso (Entusiasmo y responsabilidad); Apreciar la cultura; Criticar y ser criticado en forma constructiva (Respeto); y Valorar el trabajo en equipo para su fortalecimiento (Integración en equipo).

XI. CAMPO DE APLICACIÓN PROFESIONAL

La aplicación profesional del curso de seguridad fue diseñada para darle al alumno las herramientas teóricas para desempeñarse en cualquier empresa pública o privada. En la cual se le presenten problemáticas que involucren la protección de los medios de información, comunicación, manejo de datos, así como los valores éticos y morales que el estudiante deberá de manifestar en todo momento.

XII. EVALUACIÓN

1) ASPECTOS A EVALUAR

1) ASPECTOS A EVALUAR

a. **Participación**; en este criterio se incorporan las participaciones individuales y por equipo, las asistencia a las sesiones presénciales, la puntualidad en la entrega de los actividades de aprendizaje, así como la disposición y responsabilidad para el aprendizaje del curso
b. **Trabajos de aprendizaje**: a este rubro pertenecen la recepción, revisión y evaluación de los trabajos y actividades de aprendizaje que se desarrollaran en el curso, tales como las actividades preliminares, las de contenidos, las integradores, la participación en foros temáticos y la entrega de los productos finales.
c. **Productos de aprendizaje**; aquí se manejaran las evaluación periódicas, para las cuales se propone 2 evaluaciones parciales y la entrega de un portafolio de evidencias.

2) **MEDIOS DE EVALUACIÓN**

a. Actividades en clase o ejercicios resueltos por el alumno.
b. Trabajos de investigación (escritos y documentos).
c. Elaboración de un portafolio de evidencias; que contendrá los ejercicios hechos en clase

3) MOMENTOS DE EVALUACIÓN

Los momentos de la evaluación será continua y cada elemento suma cierto porcentaje a la calificación final del curso. Se tomaran los elementos investigación, tareas, participación en clase, examen, planteamiento y resolución de ejemplos teóricos.

4) PORCENTAJE DE CADA UNO DE LOS CRITERIOS

El criterio para obtener derecho a calificación en el periodo es:
Universidad de Guadalajara y conforme al artículo 12 los medios de evaluación y los puntajes correspondientes serán los siguientes:

I. Instrumento de evaluación para valorar los conocimientos adquiridos (examen escrito)…… 70%
II. Tareas (escrito)…….. 20%.
a) Presentación = 3%
a) Contenido = 12%
b) Redacción, referencia, bibliografía, conclusiones = 5%
III. Participación (comunicación oral y escrita)…….. 10%
Criterio de asignación
a) El alumno participa en clase y aporta conocimiento al grupo = 5%

b) El alumno es capaz de crear un portafolio de evidencia o desarrolla adecuadamente un ejercicio. = 5%

XIII. TIPO DE PRÁCTICAS

Todas las prácticas y actividades realizadas en el aula son individuales pero se permite que durante el desarrollo de las mismas puedan interactuar los alumnos con sus demás compañeros para su retroalimentación.
A la hora de entregar las tareas, realizar los exámenes y hacer su participación oral y/o escrita la evaluación es individual.

XIV. MAESTROS QUE IMPARTEN LA MATERIA

Lic. Javier Joya Lomelí.
Código: 2830345
e-mail: javier_joya@hotmail.com

Formación. Licenciado en Sistemas Computacionales, Instituto de Ciencias y Estudios Superiores de Michoacán. Estudiante de la Maestría en Administración de Instituciones Educativas, becado del Instituto Tecnológico de Monterrey, Campus Guadalajara, Educación Virtual Vía Internet (ITESM). Diplomado en Administración, Democracia y Desarrollo Municipal, UMSNH, Escuela de Economía, Edif.. "T", Ciudad Universitaria, Morelia, Mich., Diplomado en El Ciclo de Vida de los Proyectos de Inversión , OEA, UMSNH, Escuela de Economía, Edif.. "T", Ciudad Universitaria, Morelia, Mich.

Conocimientos y habilidades. Manejo de equipo de cómputo en mantenimiento preventivo, correctivo y adaptativo. Especialista en lenguajes de programación y programación orientada a objetos. Especialista en manejadores de bases de datos. Pleno conocimiento en el lenguaje de programación lógica y funcional. Programación y aplicaciones en ensamblados. Dominio de sistemas operativos basados en Windows y lynux.

XV. PROFESORES PARTICIPANTES

CREACIÓN DEL CURSO:
Lic. Javier Joya Lomelí.
MODIFICACIÓN DEL CURSO: N/A
EVALUACIÓN DEL CURSO:
Mtra. Dalila Cruz Piña / Mtro. Héctor Manuel Rodriguez Gómez

Vo. Bo.

Mtra. Dalila Cruz Piña
Presidente de la Academia de
Arquitectura y sistemas de computadoras

Dr. Aurelio Enrique López Barrón
Jefe del Departamento de Ciencias y Tecnologías de la Información y Comunicación

Dr. Jorge Ignacio Chavoya Gama
Director de la División de Ingenierías