1. Datos Generales de la asignatura

Nombre de la asignatura:	**Seguridad Informática.**
Clave de la asignatura:	**IFC-1021**
SATCA[1]:	**2 - 2 - 4**
Carrera:	**Ingeniería en Informática.**

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta al perfil del Ingeniero en Informática en las siguientes competencias:

- Aplica conocimientos científicos y tecnológicos en el área informática para la solución de problemas con un enfoque multidisciplinario.
- Formula, desarrolla y gestiona el desarrollo de proyectos de software para incrementar la competitividad en las organizaciones, considerando las normas de calidad vigentes.
- Aplica herramientas computacionales actuales y emergentes para optimizar los procesos en las organizaciones.
- Crea y administra redes de computadoras, considerando el diseño, selección, instalación y mantenimiento para la operación eficiente de los recursos informáticos.
- Se desempeña profesionalmente con ética, respetando el marco legal, la pluralidad y la conservación del medio ambiente.
- Participa y dirige grupos de trabajo interdisciplinarios, para el desarrollo de proyectos que requieran soluciones innovadores basadas en tecnologías y sistemas de información.

La asignatura de Seguridad Informática habilita al estudiante de Ingeniería Informática en los conocimientos y habilidades para diseñar e implementar normas de seguridad y estándares para el aseguramiento de los activos informáticos de las organizaciones.

Ante la apertura de los sistemas y negocios a la globalización con el uso del Internet, la asignatura de Seguridad Informática permite que el estudiante conozca los distintos medios de ataques a los que estamos expuestos para minimizarlos y las directrices actuales que le ayudarán a proteger sus recursos permitiendo la implementación de Normas y Estándares internacionales para la continuidad del negocio.

La asignatura de Seguridad Informática se encuentra estructurada de tal manera que el aprendizaje sea evolutivo en el conocimiento adquirido iniciando con los conceptos básicos de seguridad y las principales amenazas a las que se encuentran expuestos nuestros activos informáticos, posteriormente la asignatura nos permitirá conocer las directrices o temas actuales relacionados con la Seguridad que permitan conocer y tener la habilidad de aplicarlas de acuerdo a las necesidades de cada organización buscando la implementación de un Sistema de Gestión de la Seguridad de la Información basado en la Norma ISO 27001.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

Esta asignatura se imparte en el V Semestre considerando que el estudiante ya cuenta con los conocimientos adquiridos de las asignaturas de Administración de los Recursos y Función Informática, Fundamentos de Telecomunicaciones, Administración para Informática; con lo cual tiene la habilidad y capacidad de implementar normas, estándares y soluciones tecnológicas para proteger los activos de la organización alineando las estrategias de las Tecnologías de Información con las estrategias de negocio de la organización para la toma de decisiones.

Intención didáctica

Se organiza el temario agrupando los contenidos de la asignatura en cuatro temas, distribuyendo los conceptos teóricos que ayudan a lograr el adecuado entendimiento e interpretación de las prácticas que se realizarán a lo largo del curso, lo cual permitirá el óptimo desarrollo y alcance de las competencias que esta asignatura proporciona.

En el primer tema se abordan aspectos introductorios al curso, los cuales incluyen una breve introducción a la seguridad informática, el valor de la información, así como definiciones y los tipos de seguridad informática que se pueden dar, sus objetivos, incluyendo los posibles riesgos y técnicas de aseguramiento del sistema. Al estudiar cada parte, se incluyen los conceptos involucrados con ella para hacer un tratamiento más significativo, oportuno e integrado de dichos conceptos, haciendo una énfasis muy especial en la utilidad que tendrá para más adelante, tanto del desarrollo de la asignatura como de la carrera en general. Todos los apartados, en conjunto, servirán para fundamentar una visión general de la importancia que tiene y ha adquirido la seguridad en ámbitos informáticos.

El segundo tema resalta y comprende las diferentes directrices y subtemas relacionados a los aspectos de la Seguridad Informática que permitirá que los estudiantes adquieran conocimientos, habilidades y a su vez logren implementar herramientas informáticas a través de hardware y software especializados en la protección de la información y activos de la organización. Se abarcan conceptos que coadyuvan a la integración de soluciones de seguridad trascendentales para las organizaciones que les permita minimizar los riesgos que genera la globalización y la apertura al Internet.

En el tercer tema correspondiente a firewalls como herramientas de seguridad, servirá como un ejemplo y ejercicio introductorio a este importante aspecto de seguridad perimetral, incluyendo una revisión de los diferentes tipos de firewall, las ventajas que ofrece, sus limitaciones, las políticas de uso y configuración de un firewall, así como el tratamiento de los enlaces externos y la creación de lo que se denomina como una zona desmilitarizada (DMZ, por sus siglas en inglés).

El temario culmina con el estudio y conocimiento de la Norma ISO 27001:2005 teniendo como propósito principal el de proveer capacitación en los principios, conceptos y requisitos de la misma. Se inicia con el entendimiento de los orígenes y desarrollo de la familia ISO 27000 y se continúa con la aplicación general de los objetivos de control y controles que se involucran en la Norma los cuales se derivan y están directamente alineados con aquellos listados en el código de práctica ISO/IEC 17799:2005.

El enfoque sugerido para la asignatura requiere que las actividades prácticas promuevan el desarrollo de habilidades para la experimentación, tales como: identificación, manejo y control de herramientas de software especializado para seguridad en redes; planteamiento de problemas y programación de algoritmos; trabajo en equipo; asimismo, propicien procesos intelectuales como inducción-deducción y análisis-síntesis con la intención de generar una actividad intelectual compleja; por esta razón varias de las actividades prácticas se han descrito como actividades previas al tratamiento teórico de los temas, de manera que no sean una mera corroboración de lo visto previamente en clase, sino una oportunidad para conceptualizar a partir de lo observado. En las actividades prácticas sugeridas, es

conveniente que el profesor busque solamente guiar a sus alumnos para que sean ellos los que hagan la elección de los elementos a desarrollar y la manera en que los tratarán, todo esto, para que aprendan a planificar, que no planifique el profesor todo por ellos, sino involucrarlos en el proceso de planeación.
La lista de actividades de aprendizaje no es exhaustiva, se sugieren sobre todo las necesarias para hacer más significativo y efectivo el aprendizaje. Algunas de las actividades sugeridas pueden hacerse como actividad extra clase y comenzar el tratamiento en clase a partir de la discusión de los resultados de las observaciones, incluyendo posibles actividades en línea, en caso de poder contar con un sistema gestor de contenidos. Se busca partir de hacer los procesos de manera manual, para que el estudiante se acostumbre a reconocer el funcionamiento de los algoritmos, de las herramientas usadas y de las técnicas de protección y no sólo se hable de ellos en el aula. Es importante ofrecer escenarios distintos, ya sean construidos, artificiales, virtuales o naturales
En las actividades de aprendizaje sugeridas, generalmente se propone la formalización de los conceptos a partir de experiencias concretas; se busca que el alumno tenga el primer contacto con el concepto en forma concreta y sea a través de la observación, la reflexión y la discusión que se dé la formalización; la resolución de problemas se hará después de este proceso. Esta resolución de problemas no se especifica en la descripción de actividades, por ser más familiar en el desarrollo de cualquier curso. Pero se sugiere que se diseñen problemas con datos faltantes o sobrantes de manera que el estudiante se ejercite en la identificación de datos relevantes y elaboración de supuestos.
En el transcurso de las actividades programadas es muy importante que el estudiante aprenda a valorar las actividades que lleva al cabo y entienda que está construyendo su hacer futuro y en consecuencia actúe de una manera profesional; de igual manera, aprecie la importancia del conocimiento y los hábitos de trabajo; desarrolle la precisión y la curiosidad, la puntualidad, el entusiasmo y el interés, la tenacidad, la flexibilidad y la autonomía todo esto con un alto grado de honestidad y ética profesional.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Evento
Instituto Tecnológico de Saltillo del 5 al 9 de octubre de 2009.	Representantes de los Institutos Tecnológicos de: Apizaco, Cerro Azul, Chetumal, Ciudad Juárez, Ciudad Madero, Superior de Coatzacoalcos, Colima, Comitancillo, Conkal, Durango, El Llano Aguascalientes, El Salto, Superior de Fresnillo, Huejutla, Superior de Lerdo, Linares, Los Mochis, Mexicali, Morelia, Oaxaca, Superior del Occidente del Estado de Hidalgo,	Reunión Nacional de Diseño e Innovación Curricular para el Desarrollo y Formación de Competencias Profesionales de las Carreras de Ingeniería en Sistemas Computacionales, Ingeniería Informática e Ingeniería en Geociencias.

	Ocotlán, Orizaba, Piedras Negras, Pinotepa, Saltillo, San Luis Potosí, Tapachula, Tijuana, Torreón, Tuxtepec, Superior de Valladolid, Valle del Guadiana, Superior de Zacapoaxtla y Zacatecas.	
Instituto Tecnológico Superior de Poza Rica del 22 al 26 de febrero de 2010.	Representantes de los Institutos Tecnológicos de: Apizaco, Cerro Azul, Chetumal, Ciudad Juárez, Ciudad Madero, Superior de Coatzacoalcos, Colima, Comitancillo, Conkal, Durango, El Llano Aguascalientes, El Salto, Superior de Fresnillo, Huejutla, Superior de Lerdo, Los Mochis, Mexicali, Morelia, Oaxaca, Superior del Occidente del Estado de Hidalgo, Ocotlán, Orizaba, Piedras Negras, Pinotepa, Saltillo, San Luis Potosí, Tapachula, Tijuana, Torreón, Tuxtepec, Superior de Valladolid, Valle del Guadiana, Superior de Zacapoaxtla y Zacatecas.	Reunión Nacional de Consolidación de los Programas en Competencias Profesionales de las Carreras de Ingeniería en Sistemas Computacionales, Ingeniería Informática e Ingeniería Petrolera del SNEST.
Instituto Tecnológico de Querétaro del 22 al 25 de octubre de 2012.	Representantes de los Institutos Tecnológicos de: Acayucan, Campeche, Cd. Madero, Celaya, Chilpancingo, Coatzacoalcos, Colima, Ecatepec, El Grullo, Iguala, Jiquilpan, Lerdo, Los Mochis, Morelia, La Región Sierra, San Andrés Tuxtla, Sur de Guanajuato, Teziutlán, Tizimín, Zacatecas y Zitácuaro.	Reunión Nacional de Seguimiento Curricular de los Programas en Competencias Profesionales de las Carreras de Ingeniería en Sistemas Computacionales, Ingeniería Informática e Ingeniería en Tecnologías de la Información y Comunicaciones.

Instituto Tecnológico de Toluca, del 10 al 13 de febrero de 2014.	Representantes de los Institutos Tecnológicos de: Cerro Azul, Colima, Lerdo, Toluca y Veracruz.	Reunión de Seguimiento Curricular de los Programas Educativos de Ingenierías, Licenciaturas y Asignaturas Comunes del SNIT.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Desarrolla e Implementa Planes de Seguridad basado en normas y estándares internacionales para el aseguramiento de los activos de la organización y la continuidad del negocio.

5. Competencias previas

- Analiza los componentes y la funcionalidad de diferentes sistemas de comunicación para evaluar las tecnologías utilizadas actualmente como parte de la solución de un proyecto de conectividad.
- Conoce, analiza, diseña, propone y coordina proyectos informáticos en las organizaciones.
- Aplica e identifica el proceso administrativo para la gestión, diseño, evaluación e implementación de una propuesta de TIC.
- Coordina y dirige el recurso humano de un área de TIC.
- Conoce, identifica y aplica los elementos administrativos que le permitirán ubicarse y desempeñarse de manera efectiva en un contexto informático.

6. Temario

No.	Temas	Subtemas
1	Introducción a la Seguridad Informática.	1.1. El valor de la información. 1.2. Definición de seguridad informática. 1.3 Visión Global de la Seguridad Informática 1.4. Objetivos de la seguridad informática. 1.5. Posibles riesgos. 1.6. Técnicas de aseguramiento del sistema. 1.7 Principales amenazas por internet.
2	Directrices de Seguridad Informática.	2.1 Criptografía. 2.2 Esteganografía. 2.3 Certificados y Firmas Digitales. 2.4 Hacking ético. 2.5 Cómputo forense.

		2.6 IDS y IPS. 2.7 Seguridad en Linux 2.8 Seguridad en Wi-Fi.
3	Firewalls como Herramientas de Seguridad.	3.1. Tipos de firewall: de software y de hardware. 3.1.1. Firewall de capas inferiores. 3.1.2. Firewall de capa de aplicación. 3.1.3. Firewall personal. 3.2. Ventajas de un firewall. 3.3. Limitaciones de un firewall. 3.4. Políticas del firewall. 3.5. Enlaces externos.
4	Norma ISO 27001:2005.	4.1 Evolución de la familia ISO 27000. 4.2 Objetivos de control y controles. 4.2.1 Política de seguridad. 4.2.2 Organización para la seguridad de la información. 4.2.3 Administración de activos. 4.2.4 Seguridad de los recursos humanos. 4.2.5 Seguridad física y ambiental. 4.2.6 Gestión de las comunicaciones y operaciones. 4.2.7 Control de accesos. 4.2.8 Adquisición, desarrollo y mantenimiento de sistemas de información. 4.2.9 Gestión de incidentes de la seguridad de la información. 4.2.10 Gestión de la continuidad del negocio. 4.2.11 Cumplimiento.

7. Actividades de aprendizaje de los temas

1. Introducción a la Seguridad Informática.	
Competencias	Actividades de aprendizaje
Específica(s): Identifica los diferentes tipos de riesgos y amenazas que existen por internet para coadyuvar al aseguramiento de los sistemas de la organización. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Trabajo en equipo. • Capacidad de aplicar los conocimientos. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma. Autónoma. • Búsqueda del logro.	• Analizar el valor de la información en las organizaciones para identificar los activos críticos en reunión grupal y entregar resumen. • Investigar distintas definiciones de Seguridad Informática para participar y discutir en grupo y enviar documento impreso al sitio de la asignatura o vía correo electrónico. • Examinar el Diagrama de la Visión Global de la Seguridad para conocer los elementos que la conforman. • Definir los Objetivos de la Seguridad Informática y discutir su impacto en las organizaciones. • Investigar los principales riesgos informáticos que tiene una organización y entregar documento impreso. • Realizar un Análisis de Riesgo de una organización de la entidad y exponerlo en clase. • Conocer las principales amenazas por internet y aprender a identificarlas
2. Directrices de Seguridad Informática.	
Competencias	Actividades de aprendizaje
Específica(s): Analiza las distintas técnicas y directrices de la seguridad informática para implementar soluciones integradoras en la protección de	• Investigar el concepto de criptografía y la clasificación de este tipo de criptosistemas y entregar documento impreso.

los activos críticos de la organización permitiendo la continuidad del servicio. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Trabajo en equipo. • Capacidad de aplicar los conocimientos. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma. Autónoma. • Búsqueda del logro.	• Elaborar mapas conceptuales y cuadros sinópticos con la información recabada . • Desarrollar un software que simule la encriptación de una cadena de caracteres para el entendimiento de la criptografía y exponer en clase. • Investigar el concepto de Estaganografía y exponer en clase los distintos ejemplos de su aplicación. • Investigar el concepto de certificado y firma digital elaborando con ello un mapa conceptual, el cual intercambiará con sus demás compañeros. • Examinar en clase el concepto de Hacking Ético ejemplificando con una lluvia de ideas sus áreas de interés. • Instalar y evaluar distintas herramientas de seguridad en el área de Criptografía, Esteganografía y Cómputo Forense. • Valorar IDS y los IPS más comunes en el mercado y realizar un diagrama con sus ventajas y desventajas. • Investigar las principales características de la seguridad en Linux y sus herramientas más comunes y entregar documento impreso. • Determinar por lluvia de ideas las principales recomendaciones de seguridad en WiFi.
3. Firewalls como Herramientas de Seguridad.	
Competencias	Actividades de aprendizaje
Específica(s): Investiga y evalúa los diferentes tipos de firewall como método de protección de una	• Investigar qué es un firewall, para qué sirve, sus características y clasificación y exponer en clase.

red de computadoras para proteger la información de las organizaciones. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Trabajo en equipo. • Capacidad de aplicar los conocimientos. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma. Autónoma. • Búsqueda del logro.	• Plantear en sesión grupal escenarios de aplicación de un firewall. • Investigar productos comerciales y gratuitos, tanto de firewalls de software como de hardware y entregar documento impreso. • Investigar las ventajas y limitaciones de un firewall, haciendo un cuadro comparativo y luego desarrollar la misma actividad, pero analizando a los diferentes productos encontrados. • Intercambiar y discutir con los demás compañeros sus hallazgos • Verificar la manera en que un firewall maneja los enlaces externos y verificar si hay diferencia entre un firewall de hardware y uno de software en este sentido. • Instalación, configuración y administración de un firewall de hardware o de software.
4. Norma ISO 27001:2005.	
Competencias	Actividades de aprendizaje
Específica(s): Analiza el alcance y la aplicación de las normas de sistemas de gestión de seguridad de la información, así como su función para ayudar a la organización a implementarlo con efectividad, consistencia y satisfacción del cliente. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones.	• Desarrollar un diagrama de la evolución de la Familia ISO 27000 para identificar sus avances en cada versión y exponer en clase. • Comprender las definiciones y terminología del sistema de gestión de seguridad de la información. • Interpretar los requisitos de la norma ISO 27001:2005 para aplicarlos en la implantación de un sistema de gestión de seguridad de la información.

• Trabajo en equipo. • Capacidad de aplicar los conocimientos. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma. Autónoma. • Búsqueda del logro.	• Desarrollar e Implementar de manera individual un Plan de Seguridad de la Información a empresas de su entorno. Exponer en grupo el Plan de Seguridad Implementado en la organización escogida.

8. Práctica(s)

- Identificar las principales amenazas y riesgos de ataques informáticos que existen para desarrollar estudios de Análisis de Riesgos a empresas del entorno.
- Analizar en mesas de trabajo la Visión actual de la seguridad informática para identificar cada uno de sus componentes y la interrelación entre ellos.
- Analizar, Instalar y experimentar diferentes herramientas de software especializados en temas de seguridad para que de forma grupal seleccionemos la que mejores beneficios le ofrezca a las empresas de acuerdo a sus necesidades.
- Identificar en lluvia de ideas las empresas líderes en desarrollo de soluciones informáticas de seguridad.
- Realizar pruebas de ataque-defensa utilizando un conjunto de herramientas previamente seleccionadas para conocer los principales métodos de ataque a los que estamos expuestos y los mecanismos de defensa.
- Analizar e Identificar los principales firewall que existen en el mercado para conocer sus características, costos, requisitos de instalación para desarrollar soluciones a la medida.
- Instalar un firewall de software utilizando el sistema operativo Linux para conocer sus ventajas y desventajas de los dispositivos firewall de hardware.
- Seleccionar una organización o empresa del entorno para realizar en ella la implementación de un Plan de Seguridad abarcando mínimo 4 dominios de control de la Norma ISO 27001:2005 para presentarse como proyecto integrador buscando reconocer las vulnerabilidades de la organización y cómo prevenir y minimizar los riesgos.

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(s) de la asignatura, considerando las siguientes fases:

- **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.
- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.
- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de las competencias genéricas y especificas a desarrollar.
- **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de "evaluación para la mejora continua", la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación por competencias

Para evaluar las actividades de aprendizaje se recomienda solicitar: mapas conceptuales, reportes de prácticas, estudios de casos, exposiciones en clase, ensayos, problemarios, reportes de visitas, portafolio de evidencias y cuestionarios, cuadro sinóptico.

Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, listas de verificación, matrices de valoración, guías de observación, coevaluación y autoevaluación.

11. Fuentes de información

Impresas:

1. Aguirre, Jorge R. (1999) "Aplicaciones Criptográficas." Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España.
2. PPSILON, (2011)"Seguridad informática - Ethical Hacking" Edit ACISSI
3. Kaufman, Charlie; Perlman, Radia; Spencer, Mike. "Network Security: Private Communication in a Public World". Prentice Hall.
4. Garcia-Cerevignon A. Alegre Ramos M. (2010) ,"Seguridad Informática" Edit PARANINFO
5. Cheswick, William R.; Bellovin, Steven M. "Firewalls and Internet Security: Repelling the Wily Hacker." Addison-Wesley Pub Co.
6. Cano-Barrón, José E.; Martínez-Peláez, Rafael; Soriano, Miquel. (2007) "Current Problems and Challenges in Developing a Standard Digital Rights Management System". 5th International

Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods (incorporating the 3rd International ODRL Workshop). Koblenz, Alemania.
7. Lucena López, Manuel J. (2007). "Criptografía y Seguridad en Computadores". Cuarta Edición. Criptografía y Seguridad en Computadores es un libro electrónico en castellano, publicado bajo licencia Creative Commons.
8. Anónimo. "Máxima Seguridad en Linux".Prentice Hall.
9. Norma ISO 27001:2005.

Digitales:
10. Aguirre, Jorge R. "Libro Electrónico de Seguridad Informática y Criptografía". (2006); Depósito Legal M-10039-2003. Disponible en Internet en http://www.criptored.upm.es/guiateoria/gt_m001a.htm
11. Zimmermann, P. (1999), "An Introduction to Cryptograpy". Network Associates. available at: ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf