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.

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. 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.

4. 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.

5. 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.