1. DATOS DE LA ASIGNATURA

Nombre de la asignatura:	**Gestión de la Seguridad de la información**
Carrera:	**Ingeniería en Tecnologías de la Información y Comunicaciones**
Clave de la asignatura:	**GTF-2105**
SATCA	**3-2-5**

2. HISTORIA DEL PROGRAMA

Lugar y fecha de elaboración o revisión	Participantes	Observaciones (cambios y justificación)
Instituto Tecnológico de Culiacán 30 abril 2021	M.C. Luis Ernesto Lizárraga Bolaños MGTI. Norma Rebeca Godoy Castro Lic. Pedro Villa Casas M.C. Nora E. Cancela García MTI. María del Rosario González Álvarez	Elaboración de la asignatura: Gestión de Tecnologías de Negocios.

3. PRESENTACIÓN

Caracterización de la asignatura:

En esta "era de la información" la información ha llegado a ser uno de los activos más valiosos para las empresas por lo cual es necesario desarrollar procesos e implantar políticas que garanticen su seguridad. El Ingeniero en TIC debe por lo tanto no sólo utilizar tecnología sino tener una visión global que le ayude a entender el papel que juega esta para salvaguardar la información y los procesos que dependen de ella. Esta materia está relacionada con la materia de Administración y seguridad de redes, Auditoría en tecnologías de la información.

Intención didáctica:
El temario se organiza en seis unidades, las cuales incluyen contenidos conceptuales y de aplicación de los mismos a través de casos prácticos.

En la primera unidad se introduce el problema de la seguridad de la información como una parte vital de los procesos de negocios.

En la segunda unidad se identifican las fases para la planeación de la seguridad, la

planeación de contingencias y se definen las políticas que ayuden a reforzar la seguridad.

En la tercera unidad se analizan los diferentes modelos de arquitectura de la seguridad, así como los de gestión que permitan al alumno crear un marco de referencia y utilizar las mejores prácticas de la industria.

En la unidad cuatro se identifican y evalúan los riesgos a los que se ve expuesta la información, al mismo tiempo que se diseñan estrategias para disminuirlos y mitigar su efecto.

En la unidad cinco se evalúan y seleccionan las tecnologías adecuadas de acuerdo los riesgos de seguridad que se requieran mitigar.

Por último, en la unidad seis se abordan los aspectos éticos y legales de la seguridad de la información para concientizar al alumno sobre su responsabilidad con la sociedad.

4. COMPETENCIAS A DESARROLLAR:

Competencia general:

Diseñar medidas preventivas y reactivas que garanticen la confiabilidad de la información aplicando procedimientos, técnicas y tecnología.

Competencias específicas:

- Identificar los aspectos más importantes de la seguridad de la información para considerarlos en un proyecto de gestión de la seguridad
- Diseñar planes y políticas de seguridad de la información con visión corporativa.
- Identificar los diferentes modelos de gestión para seleccionar el que mejor se adapte a las necesidades de la empresa.
- Evaluar los riesgos a los que se expone la información para tomar medidas que ayuden a reducir el impacto de incidentes.
- Utilizar diferentes tecnologías que ayuden reforzar la seguridad de la información
- Actuar en forma ética y legal para salvaguardar la información de la empresa.

Competencias genéricas:

Competencias instrumentales:

- Capacidad de organización y planificación.
- Comunicación oral y escrita.
- Solucionar de problemas utilizando una metodología.
- Tomar de decisiones de manera razonada

Competencias interpersonales

- Capacidad crítica y autocrítica.
- Trabajo en equipo.
- Habilidad en las relaciones interpersonales
- Compromiso ético

Competencias sistémicas

- Aplicar los conocimientos, métodos

	y herramientas a situaciones concretas reales. • Liderazgo • Diseño y gestión de proyectos

5. COMPETENCIAS PREVIAS

- Diseñar, instalar y administrar redes de cómputo y comunicaciones, bajo modelos y estándares internacionales, para satisfacer las necesidades de la información de los sistemas sociales, garantizando aspectos de seguridad y calidad.

6. TEMARIO

Unidad	Temas	Subtemas
1	Introducción a la seguridad de la información	1.1 Conceptos 1.1 Seguridad 1.1 Modelo de seguridad 1.1 Gestión 1.2 Principios de la administración de seguridad de la información 1.2 Planeación 1.2 Políticas 1.2 Programas 1.2 Protección 1.2 Gente 1.2 Gestión de proyectos 1.3 Gestión de proyectos 1.3 Gestión de proyectos de seguridad 1.3 Herramientas para la gestión de proyectos
2	Políticas y planeación de la seguridad	2.1 Planeación de la seguridad 2.1.1 El rol de la planeación 2.1.2 Precursores de la planeación 2.1.3 Planeación estratégica 2.1.4 Gobierno de la seguridad de la información 2.1.5 Planeación de la implantación 2.2 Planeación de contingencias 2.2.1 Análisis del impacto

		organizacional 2.2.2 Plan de respuesta a incidentes y desastres 2.2.3 Plan de continuidad del negocio 2.2.4 Pruebas del plan de contingencias 2.3 Políticas 2.3.1 Justificación 2.3.2 Desarrollo de políticas 2.3.3 Distribución de políticas 2.3.4 Conformidad de políticas 2.3.5 Aplicación de políticas 2.3.6 Herramientas
3	Modelos de gestión de seguridad	3.1 Modelos de arquitectura de la seguridad 3.1.1 Trusted computing base 3.1.2 TSEC 3.1.3 Common Criteria 3.1.4 Otros 3.2 Modelos de gestión de la seguridad 3.2.1 ISO 27000 3.2.2 COBIT 3.2.3 Modelo de seguridad del NIST 3.2.4 ITIL 3.2.5 Otros 3.3 Prácticas de gestión de la seguridad 3.3.1 Benchmarking 3.3.2 Medición del desempeño 3.3.3 Certificación y acreditación
4	Gestión de riesgos	4.1 Introducción 4.2 4.2 Identificación de riesgos 4.3 Evaluación de riesgos 4.4 Estrategias de control de riesgos 4.5 Análisis de factibilidad y costo beneficio 4.6 Prácticas recomendadas de control de riesgos 4.6.1 OCTAVE 4.6.2 Enfoque de gestión de riesgos Microsoft 4.6.3 FAIR 4.6.4 ISO-27005
5	Tecnologías	5.1 Control de acceso 5.2 Firewalls

		5.3 Sistemas de detección/prevención de intrusos 5.4 Protección de acceso remoto 5.5 Protección de redes inalámbricas 5.6 Herramientas de rastreo y análisis 5.7 Criptografía
6	Ética y legislación	6.1 Introducción 6.2 Legislación 6.2.1 Leyes internacionales 6.2.2 Legislación local y nacional 6.3 Ética 6.3.1 Ética y educación 6.3.2 Disuasión de comportamiento no ético e ilegal 6.4 Organizaciones profesionales y sus códigos de ética 6.4.1 ACM 6.4.2 (ISC)2 6.4.3 SANS 6.4.4 ISSA

7. SUGERENCIAS DIDÁCTICAS PARA EL DESARROLLO DE COMPETENCIAS ESPECÍFICAS

Competencias específicas[5]	Actividades de aprendizaje
Identificar los aspectos más importantes de la seguridad de la información para considerarlos en un proyecto de gestión de la seguridad	• Elaborar un mapa conceptual que muestre los principios de la gestión de la seguridad. • Desarrollar un proyecto a lo largo del curso en donde aplique los conocimientos que se adquieren.
Diseñar planes y políticas de seguridad de la información con visión corporativa	• Elaborar un mapa mental que muestre la importancia de la planeación de un proyecto • Diseñar el plan de contingencias para el proyecto. • Diseñar las políticas y definir cómo aplicarlas para el proyecto
Identificar los diferentes modelos de gestión para seleccionar el que mejor se adapte a las necesidades de la empresa.	• Analizar los modelos y seleccionar el que más se adapte a las necesidades del proyecto
Evaluar los riesgos a los que se expone la información para tomar medidas que ayuden	• Identificar y evaluar, en algún escenario, los diferentes riesgos

a reducir el impacto de incidentes.	que se pueden presentar. • Diseñar estrategias de control de riesgos para el caso seleccionado • Realizar el estudio de factibilidad para la estrategia de control de riesgos diseñada • Aplicar lo aprendido en el proyecto
Utilizar diferentes tecnologías que ayuden reforzar la seguridad de la información	• Seleccionar y utilizar las tecnologías más adecuadas para el proyecto
Actuar en forma ética y legal para salvaguardar la información de la empresa.	• Realizar un ensayo sobre la ética en la seguridad de la información y el proyecto. • Investigar los aspectos legales que impactan al proyecto.

8. SUGERENCIAS DIDÁCTICAS PARA EL DESARROLLO DE COMPETENCIAS GENÉRICAS.

- Utilizar, como apoyo, casos de estudio que puede sacar de la bibliografía complementaria
- Definir proyectos que busquen resolver problemas de seguridad en las empresas reales o ficticias.
- Desarrollar prácticas dinámicas que pongan de manifiesto la importancia de la seguridad de la información.
- Traer a discusión o debate artículos o noticias actuales relativas a la seguridad de la información.

9. SUGERENCIAS DE EVALUACIÓN

Diagnóstica	Formativa	Sumativa
Realizar un cuestionario que ayude a evaluar el conocimiento de su carrera	Presentación de avances del proyecto	3 exámenes parciales Proyecto Presentación del proyecto

10. FUENTES DE INFORMACIÓN

Libro de texto

- Michael E. Whitman; Herbert J. Mattord, Management Information Security, Course Technology, 3 edition, 2010

Lecturas complementarias

- Michael E. Whitman; Herbert J. Mattord; Readings and Cases in the Management of Information Security, Course Technology, 1 edition, 2005
- Michael E. Whitman; Herbert J. Mattord, Hands-On Information Security Lab Manual, Course Technology, 3 edition, 2010
- Gómez Vieites, A. (2007). Enciclopedia de la seguridad informática. México: Alfaomega. ISBN:678-970-151-266-1

11. PERFIL DEL PROFESOR QUE IMPARTIRÁ LA MATERIA

- Lic. En Informática, maestro o doctor en ciencias de la computación o área afín, con experiencia práctica en el área de seguridad de la información, Conocer la serie 27000 de las normas ISO y Dominar herramientas de seguridad