1. Datos Generales de la asignatura

Nombre de la asignatura:	**Gestión de la Seguridad en Redes**
Clave de la asignatura:	**NVD-2305**
SATCA[1]:	**2-3-5**
Carrera:	**Ingeniería en Tecnologías de la Información y Comunicaciones**

2. Presentación

Caracterización de la asignatura

Esta materia permitirá al egresado identificar, diseñar, administrar y evaluar aspectos de seguridad y calidad de las redes en el ámbito de los negocios y de ahí fomentar la aplicación de políticas, procedimientos, prácticas y estructuras organizacionales que permitan evaluar constantemente la función de las redes y optimizar su potencial para las organizaciones, al mismo tiempo que las mantienen a salvo y proveer una garantía razonable de que sean alcanzados los objetivos y la continuidad del negocio. En esta asignatura se tiene la intención de formar profesionistas capaces de implementar sistemas de seguridad bajo políticas internas de las organizaciones y estándares aceptados.

Intención didáctica

Esta asignatura pretende que el estudiante analice la normatividad y estándares existentes, que, aplicados en el ámbito de la seguridad en el uso de las tecnologías de la información, permitan la disponibilidad de los servicios de TI desarrollando planes de continuidad del negocio y de recuperación de desastres. La seguridad es un proceso continuo dentro de la ingeniería del software que requiere del conocimiento y aplicación de las técnicas apropiadas para evitar las posibles vulnerabilidades.

Para ello, se organiza el temario en cinco unidades. La primera unidad abarca la necesidad de seguridad en la vida cotidiana hasta el ámbito de las redes, en la segunda unidad determinará la gestión de la seguridad de las redes, involucrando a partir de establecer el responsable de la seguridad de las redes, el manejo de la arquitectura de seguridad con base en métricas de la seguridad para aplicar una metodología de gestión del riesgo integrando lo necesario a partir de una auditoría de seguridad de redes, conocerá la seguridad del software a detalle verificando desde un código malintencionado, la denegación del servicio y determinando la estrategia de protección multinivel.

En la tercera unidad se identifican los riesgos para determinar el proceso de administración del mismo; en la cuarta unidad se establecen y mantienen acciones que buscan cumplir los requerimientos de seguridad, calidad, servicio y capacidad.

El quinto, se enfoca en el concepto y arquitectura de las redes de nueva generación,

[1] Sistema de Asignación y Transferencia de Créditos Académicos

servicios y aplicaciones en la sociedad, así como los aspectos regulatorios y económicos de las redes nueva generación. Se sugiere que en esta unidad se realicen actividades integradoras, desarrollando prácticas donde se requiera involucrar los diferentes conceptos en ejercicios, utilizando equipo y simuladores. 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 a partir del análisis de las soluciones propuestas.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico del Altiplano de Tlaxcala, del 16 agosto al 30 de Septiembre de 2021.	La Academia de Tecnologías de la Información y Comunicaciones del Instituto Tecnológico del Altiplano de Tlaxcala Participantes: ● Lic. Jesús Zavala Galicia. ● Mtro. Yimi Zainos Cuapio. ●Ing. Yovani Guevara Cortes. ●Ing. Eleazar Juárez Hernández ●Ing. Francisco Javier Altamirano Juárez	Diseño y elaboración de la materia de Gestión de la Seguridad en Redes, en la especialidad de Nuevas Tecnologías.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Conoce y aplica tecnologías y herramientas de las tecnologías de seguridad para atender necesidades acordes al entorno. Interpreta normas y estándares de seguridad con la finalidad de diseñar un esquema básico de seguridad que permita la protección de los recursos en la red, con la intención de preservar la confidencialidad, integridad y disponibilidad de los elementos que la tratan. Identifica los conceptos básicos para analizar la seguridad en las redes. Identifica riesgos con el fin de trabajar estándares para lograr la seguridad en las Redes. Diagnostica el nivel de inseguridad mediante la aplicación de métodos y análisis de riesgos. Analiza una metodología apropiada para desarrollar y documentar la seguridad en las Redes. Identifica riesgos con el fin de trabajar estándares para lograr la seguridad en las Redes.

Diagnostica el nivel de inseguridad mediante la aplicación de métodos y análisis de riesgos.

5. Competencias previas

Es necesario que el estudiante tenga aprendizaje previo respecto a Programación Orientada
a Objetos, Ingeniería de Software, Redes emergentes y Tecnologías Inalámbricas.
● Comprensión de lectura.
● Capacidad de aprender y mantenerse actualizado.
● Obtener las capacidades de diseño con las tecnologías de la información para ayudar a los individuos, grupos y organizaciones a alcanzar sus metas.
● Poseer habilidades de comunicación tanto oral como escritas necesarias para el diseño y gestión de los sistemas de información.
● Analiza una metodología apropiada para desarrollar y documentar un sistema de administración de la seguridad.
● Identifica riesgos con el fin de trabajar estándares para lograr la seguridad en las Redes.
● Diagnostica el nivel de inseguridad mediante la aplicación de métodos y análisis de riesgos
● Capacidad de aprender y mantenerse actualizado.
● Poseer habilidades de comunicación tanto oral como escrita necesaria para el diseño y gestión de los sistemas de información.
● Trabaja colaborativamente para el desarrollo de tareas, proyectos con actitud constructiva apoyándose en el uso de las TIC´s.
● Observar el escenario problema e identificar oportunidades de desarrollo de proyectos
generando ideas innovadoras de la aplicación de la investigación en su área profesional.
● Propone maneras de solucionar un problema o desarrollar un proyecto en equipo, definiendo un curso de acción con pasos específicos.

6. Temario

No.	Temas	Subtemas
1	**Fundamentos de seguridad en redes**	1.1 Seguridad en la vida cotidiana. ● Concepto general. ● Importancia. 1.2 Perspectivas de la seguridad en las redes. ● Confidencialidad, integridad y disponibilidad. ● Servicio fiduciario. 1.3 Términos relacionados con la seguridad (Activo de información, amenaza, impacto, riesgo, vulnerabilidad, ataque, incidente, política). 1.4 Problemas comunes de seguridad en redes. 1.4.1 Tipos de ataques. ● Pasivos (Intercepción).

		● Activos: (Interrupción, fabricación, modificación). 1.4.2 Los atacantes. ● Hackers. ● Crackers. ● Intrusos. 1.4.3 Causas y motivaciones de los ataques informáticos.
2	**Gestión de la seguridad de las redes**	2.1 El responsable de la seguridad de la información. 2.2 Seguridad en redes. 2.3 Metodologías de Gestión del Riesgo.
3	**Esquemas y modelos de seguridad**	3.1 Misión de seguridad. 3.2 Grupo de elaboración de políticas. 3.3 Política de seguridad. 3.4 Procedimientos de seguridad. 3.5 Especificación de mecanismos de seguridad. 3.6 Implementación y estándares. 3.7 Modelos de seguridad.
4	**Análisis del riesgo**	4.1 Evaluación del riesgo. 4.2 Determinación de la probabilidad. 4.3 Número de ocurrencias del evento en un periodo de un año. 4.4 Identificación de vulnerabilidades. 4.5 Identificación de controles. 4.6 Plan de implementación tecnológica 4.7 Análisis funcional de políticas. 4.8 Análisis funcional de procedimientos. 4.9 Análisis funcional de estándares. 4.10 Interpretación de los resultados. 4.11 Determinar medidas de seguridad. 4.12 Documentación del proceso de análisis de los riesgos.
5	**Redes de próxima generación (NGN)**	5.1 Concepto y Arquitectura de NGN. 5.2 Servicios y aplicaciones sobre NGN. 5.3 Aspectos técnicos de NGN. 5.4 Modelos de migración de servicios PSTN a NGN. 5.5 Aspectos económicos y regulatorios de NGN.

7. Actividades de aprendizaje de los temas

Unidad 1: Fundamentos de seguridad en redes.	
Competencias	Actividades de aprendizaje
Específica(s): Identifica los conceptos básicos para analizar los sistemas de seguridad de redes. Genéricas: Propiciar actividades de búsqueda, selección y análisis de información en distintas asignaturas.	● Elaborar fichas bibliográficas sobre los conceptos de seguridad de TI. ● Elaborar cuadros sinópticos comparativos sobre los conceptos investigados, tomando en cuenta las fichas bibliográficas.
Unidad 2: Gestión de la seguridad de las redes.	
Competencias	Actividades de aprendizaje
Específica(s): Integrar la arquitectura de seguridad mediante el uso de métricas y la aplicación de una metodología de gestión del riesgo. Genéricas: Fomentar actividades grupales que propicien el intercambio de ideas, reflexión, integración y colaboración entre los estudiantes.	● Identifica amenazas, vulnerabilidad y riesgos. ● Elaborar un reporte diagnóstico de riesgos basada en el impacto dentro de una organización ● Elaborar un reporte diagnóstico.
Unidad 3: Esquemas y modelos de seguridad.	
Competencias	Actividades de aprendizaje
Específica(s): Indaga y analiza los diferentes modelos relevantes en el ámbito de seguridad de redes para comprender y mejorar las buenas prácticas. Genéricas: Desarrollar actividades de aprendizaje que propicie la aplicación de las metodologías y planes de respuesta a contingencia que se van presentando en el desarrollo de la asignatura.	● Describir la estructura de los estándares aplicados a la seguridad, analizando su importancia en la actualidad. ● Reconocer distintos modelos aplicables a la seguridad. ● Buscar, seleccionar y organizar información de diferentes fuentes, acerca de los mecanismos utilizados para salvaguardar la seguridad en redes.
Unidad 4: Análisis de riesgo.	
Competencias	Actividades de aprendizaje
Específica(s): Identifica riesgos con el fin de trabajar estándares para lograr la seguridad en las redes. Genéricas: Fomentar actividades grupales que propicien el intercambio de ideas, reflexión, integración y colaboración entre los estudiantes.	● Identificar amenazas, vulnerabilidad y riesgos. ● Elaborar un reporte diagnóstico de riesgos basada en el impacto dentro de una organización ● Realizar una propuesta de administración de riesgos. ● Realizar un proceso de monitoreo y administración de riesgos a partir de evaluar su estado e impacto para determinar la tolerancia del mismo.
Unidad 5: Redes de próxima generación (NGN).	
Competencias	Actividades de aprendizaje
Específica(s): Identifica las características de las redes de próxima generación y su impacto en la vida moderna para proponer soluciones vanguardistas. Genéricas: Desarrollar actividades de	● Uso de un portal de Internet para apoyo didáctico de la materia. ● Ejercicios en clase para solución de problemas de NGN ● Desarrollar escenarios en clase para

aprendizaje que propicie la aplicación de las metodologías y planes de respuesta a contingencia que se van presentando en el desarrollo de la asignatura.	generar intercambio, discusiones y conclusiones ● Uso de hardware y software para realización de prácticas de NGN.

8. Práctica(s)

● Analizar la aplicación de conceptos, usando un mapa conceptual que contribuya a consolidar la comprensión y relación de los conceptos de la unidad 1, con el uso de las redes.
● Presentar el escenario de un incidente de seguridad real o ficticio, determinando los tipos de ataque presentados, así como las amenazas identificadas.
● Extraer la información relevante de un caso de estudio para diagnosticar los factores de riesgo que determinaron la situación del problema.
● Realizar el diseño de un modelo de seguridad a partir de las especificaciones de un estándar.
● Identificar las principales amenazas y riesgos de ataques informáticos que existen para desarrollar estudios de Análisis de Riesgos a empresas del entorno.
● Examinar, instalar y experimentar diferentes herramientas de software especializados en temas de seguridad en redes para que de forma grupal seleccionen la que ofrezca mejores beneficios.
● Identificar en lluvia de ideas las empresas líderes en desarrollo de soluciones informáticas de seguridad en redes.
● 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 firewalls que existen en el mercado para conocer sus características, costos, requisitos de instalación para desarrollar soluciones a la medida en la seguridad de Redes.
● Seleccionar una organización o empresa del entorno para realizar en ella la implementación de un Plan de Seguridad para presentarse como proyecto integrador buscando reconocer las vulnerabilidades de la organización y cómo prevenir y minimizar los riesgos en una red.

9. Proyecto de asignatura

Al finalizar el programa los participantes aplicarán las diferentes tecnologías y modelos de la seguridad informática y computacional en los sistemas y redes de telecomunicaciones, considerarán las ventajas y problemáticas asociadas con el diseño y administración de políticas y mecanismos de seguridad para los recursos informáticos en los sistemas y redes de telecomunicaciones, diseñarán un proyecto de seguridad informática relacionado con una problemática real o de algún otro caso de estudio propuesto en el curso y reafirmarán sus conocimientos básicos de teoría de sistemas y redes de telecomunicaciones.

10. Evaluación por competencias

En este punto, la evaluación debe ser continua y permanente por lo que se debe considerar el desempeño en cada una de las actividades de aprendizaje, se recomienda que el alumno cuente con un portafolio de evidencias constituido por:

- Mapa mental
- Mapa conceptual
- Reporte de investigación con diferentes referencias.
- Informes y reportes de desempeño.
- Participación en clase.
- Prácticas realizadas en laboratorio.
- Información obtenida durante las búsquedas encomendadas.
- Evaluación de unidades de aprendizaje basada en casos.
- Autoevaluación, coevaluación y evaluación de las actividades.
- Examen analítico y crítico de teorías
- Hoja diagnóstica de ideas principales
- Productos elaborados en pequeños grupos, proyectos, propuestas.

Estos productos serán evaluados por medio de las rúbricas y / o listas de cotejos

11. Fuentes de información

[1] Gómez Vieites, A. (2011). Enciclopedia de la Seguridad Informática. Madrid, España: Alfaomega RA-MA

[2] Psilon, A. (2011) “Seguridad informática - Ethical Hacking” Ed. ACISSI

[3] García. C., Alegre A. (2010),” Seguridad Informática” Ed.

[4] Cordobés, Enrique, “Características generales de la criminalidad informática en Cuba”, AR: Revista de Derecho Informático, núm. 098, septiembre de 2006, http://www.alfa-redi.org/rdiartículo.shtml?x=7178.

[5] Comer, Douglas E. Interconectividad de Redes con TCP/IP Vol. I. Principios Básicos y Arquitectura. 3a. Edición. México. Ed. Prentice Hall, 2000.

[6] Halsall, Fred. Data Communications, Computer Networks and Open Systems. 4th Edition. Essex. Ed. Addison-Wesley. 1996.

[7] Sohraby, K. Miloni, D, Znati, T. (2007) Wireless Sensor Networks. Technology, protocols and applications. Wiley.

[8] ITU-T Recommendation I.130 (1988). Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN. Ed. ITU 1993. Ginebra.