1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad Digital
Clave de la asignatura:	GIB-2004
SATCA[1]:	1-4-5
Carrera:	Ingeniería Informática.

2. Presentación

Caracterización de la asignatura
Esta asignatura permite al Ingeniero Informático tener una visión general acerca de la importancia que tiene el día de hoy la protección de los datos personales en posesión de particulares, adentrándolo en un visión más amplia acerca de las responsabilidades que a su cargo tiene cuando se protegen datos de manera lógica y física dentro de las organizaciones, considerando diferentes metodologías que pueden ser aplicadas en ambientes reales y lo coloca en escenarios reales donde los principales fraudes informáticos se gestan. Esta materia aporta al perfil del profesionista la visión de los aspectos que influyen en la seguridad informática. También proporcionará los conocimientos intermedios de seguridad para el desarrollo de proyectos de tecnologías de información. La asignatura de *Seguridad Digital* tiene aportación directa al perfil de egreso debido a que, aplica conocimientos científicos y tecnológicos en el área informática para la solución de problemas con un enfoque multidisciplinario, aplica herramientas computacionales actuales y emergentes para optimizar los procesos en las organizaciones, realiza consultorías relacionadas con la función informática para la mejora continua de la organización. La importancia de esta asignatura radica en que permitirá al alumno egresar con una visión actualizada de las principales técnicas de protección contra diferentes ataques de hackers, además promueve en el alumno la necesidad de la constante actualización antes los diferentes cambios que pasan en el área de las tecnologías de la información, permitiendo así que el estudiante al final del curso pueda analizar desde un ambiente neutro las necesidades existentes en el área de seguridad digital, ayudando a mejorar sus procesos de transmisión de datos en los diferentes medios de comunicación manejados en las organizaciones. La asignatura de Seguridad Digital consta de cuatro temas, en el primer tema que lleva por título *Conceptos Generales De La Seguridad Digital*, se definen los tópicos generales sobre ciberseguridad considerando que se abordan dos elementos importantes que son la seguridad lógica de los datos y la seguridad física además de conocer las normas a

1 Sistema de Asignación y Transferencia de Créditos Académicos

las cuales están sometidos los datos personales cuando se utilizan plataformas digitales. En el segundo tema que lleva por título *Vulnerabilidades Ciberneticas e Impactos*, pretende dar a conocer las principales debilidades que pueden existir de los sistemas informáticos, así como las contramedidas que se pueden tomar para evitar los diversos tipos de ataques. El tercer tema nombrado *Pruebas de Penetración e Informática Forense* busca proveer a los alumnos de herramientas lógicas y físicas que le ayuden en la resolución de un caso forense informático, así como dar a conocer las metodologías más utilizadas en México para la realización del levantamiento de evidencias en una escena del crimen *Informática para Negocios,* busca que el estudiante aplique los conocimientos adquiridos en la asignatura al desarrollar en formato de proyecto una propuesta de gestión informática aplicada a una organización. Cabe mencionar que el tema cinco se desarrollará simultáneamente con las demás asignaturas que integran la especialidad, motivo por el cual el tema cinco es idéntico en cada asignatura.

Esta asignatura tiene relación directa con otras asignaturas del plan de estudios de Informática como lo son, *Administración De Los Recursos Y Función Informática* en el tema 5 denominado Estandarización En La Función Informática el cual pretende alcanzar la competencia de, Identificará y seleccionará los elementos necesarios para la organización física de un centro de cómputo considerando las normas de seguridad aplicables, además de la materia de Auditoria Informática en tema 4 nombrado como Auditoria De Redes, con la competencia Conocer, Identificar y seleccionar los requerimientos y estándares para una auditoría de redes que se deben considerar para determinar el nivel de aplicación en la administración, instalación, operación, seguridad, así como del personal responsable, además con el tema 5 titulado Auditoria En Telecomunicaciones y la competencia asociada de Conocer, Identificar y seleccionar los requerimientos y estándares para una auditoría de las telecomunicaciones que se deben considerar para determinar el nivel de aplicación en la administración, instalación, operación, seguridad, así como del personal responsable, y por último con la materia de *Seguridad Informática* en el tema 6 denominado Vigilancia De Los Sistemas De Información donde se cubre la competencia de Llevar al cabo una vigilancia e implementar medidas de seguridad efectivas de la información que circula a través de una red.

Intención didáctica

El temario está organizado en cuatro temas. En el primer tema se abordan los conocimientos básicos de la seguridad digital, los cuales se tienen un enfoque teórico-practico para los alumnos y una extensión y profundidad que puede ser determinada por el docente particularizando en contextos de aprendizaje que permitan tener una visión clara a los estudiantes de la importancia que tiene el estudio de la materia, además se sugiere el desarrollo de actividades que permitan el estudio de los conceptos primordiales y que a su vez puedan ser reforzados mediante practicas propuestas en sitios de seguridad que publican constantemente fallos de seguridad a nivel de sistemas operativos, se sugieren sean trabajadas las competencias genéricas de: Capacidad de análisis y síntesis, Capacidad de organizar y planear y aplicar conocimientos a la práctica.

Se sugiere abordar el segundo tema comenzando con un ejemplo práctico de la radiografía de un ataque informativo vigente durante el año que se curse la materia, esto

con la finalidad de conocer las herramientas utilizadas por los ciberdelincuentes para esconder su rastro a través de internet y visualizar la forma en que pueden explotar una vulnerabilidad, cuando es encontrada en un sistema de información, la extensión y profundidad del tema se sugiere que sea manera que se puedan analizar al menos tres ataques distintos ubicados diversas categorías de riesgo, sugiriendo el desarrollo de actividades complementarias en plataformas digitales gratuitas y que permitan al alumno capacitarse para la presentación de alguna certificación en tiempos posteriores al estudio del curso, las competencias genéricas a trabajar en este tema serian, capacidad de organizar y planificar, trabajo en equipo, habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas, solución de problemas, y capacidad de crítica y autocritica.

Es sugerible que el tema tres se aborde de una manera diferente a los demás temas, sugiriendo actividades netamente prácticas para la clara comprensión de los conceptos a estudiar, la extensión y profundidad de los temas es importante ya que un análisis forense digital conlleva una metodología estricta y apegada a normas que pueden estar tipificadas en códigos de un estado o país, es por ello que se recomienda la realización de actividades donde el docente revise de manera pulcra el levantamiento de evidencias, exponiendo los principales errores que se pueden cometer al momento de realizar de dicha actividad, las competencias genéricas a trabajar en este tema son, capacidad de aplicar los conocimientos en la práctica, habilidades en el estudio y manejo de las TI emergentes, capacidad de trabajar en equipo interdisciplinario y conocimiento en una segunda lengua.

Finalmente se recomienda abordar el tema cuatro según el enfoque de un proyecto de asignatura, mismo que conjuntará los conocimientos analizados en las cinco asignaturas que integran la especialidad, y se integra la participación de la materia de Plataformas para el Análisis y Visualización y Gestión de Datos en la realización de un proyecto común que permita evaluar el último tema de cada temario con un proyecto co-evaluativo para medir el desempeño del alumno en estas materias del cierre de la retícula de carrera de Ingeniería Informática. También se sugiere que la extensión y profundidad sobre el tema cinco sea mayor en cuanto a contenido y tiempo pues será el tema que culmina el ser de la especialidad. Las actividades sugeridas para el estudiante constan en la presentación de la construcción de un repositorio de datos, propuesta lógica de seguridad informática y desarrollo de una presentación visual de los datos utilizando plataformas libres o licenciadas, Las competencias genéricas que se buscan alcanzar en este tema son: Capacidad de análisis y síntesis, Capacidad de organizar y planificar, Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas), Solución de problemas y Toma de decisiones.

El papel que debe desempeñar el docente durante la impartición de la asignatura es el de facilitador de conocimiento, generando entornos de aprendizajes que se acerquen a lo que el alumno puede enfrentar en ambientes laborales una vez que terminen la carrera, además a brindar las herramientas y capacitación que ayuden a desarrollar las diversas practicas a lo largo del curso.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico de Estudios Superiores de Chalco Enero 2020.	Tecnológico de Estudios Superiores de Chalco. Villanueva Valdivia Guadalupe Nayelli, Romero Castro Raúl, Ramirez Vite Kevin Gyovani, Docentes de la carrera de Ingeniería Informática.	Reunión para el diseño curricular de la nueva especialidad, de la carrera de Ingeniería Informática, "Gestión Informática para Negocios".

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Analiza, diseña, desarrolla e implementa planes de seguridad lógica y pruebas de penetración basadas en normas vigentes para el aseguramiento de los activos digitales utilizados en empresas o negocios.

5. Competencias previas

- Identifica y seleccionará los elementos necesarios para la organización física de un centro de cómputo considerando las normas de seguridad aplicables.
- Conoce, Identificar y seleccionar los requerimientos y estándares para una auditoría de redes que se deben considerar para determinar el nivel de aplicación en la administración, instalación, operación, seguridad, así como del personal responsable
- Conoce, Identificar y seleccionar los requerimientos y estándares para una auditoría de las telecomunicaciones que se deben considerar para determinar el nivel de aplicación en la administración, instalación, operación, seguridad, así como del personal responsable
- Lleva al cabo una vigilancia e implementar medidas de seguridad efectivas de la información que circula a través de una red.

6. Temario

No.	Temas	Subtemas
1	Conceptos Generales De La Seguridad Digital	1.1 Conceptos básicos de la seguridad digital. 1.1.1 Seguridad física 1.1.2 Herramientas física. 1.1.3 Seguridad lógica.

		1.1.3.1 Ciberseguridad 1.1.3.2Herramientas lógicas. 1.1.4 Principios de seguridad de la información. 1.2 Políticas vigentes aplicadas a la seguridad digital en México. 1.3 Servicios de seguridad. 1.4 Medidas de aseguramiento del sistema lógico de datos. 1.5 Ética, derecho y política en el ciberespacio. 1.6 Caso de estudio (caso practico).
2	Vulnerabilidades Cibernéticas E Impactos.	2.1 Radiografía de un ataque informático 2.2 Tipos de vulnerabilidades cibernéticas. 2.2 ¿Cómo los piratas informáticos cubren sus huellas? (antiforense). 2.3.1¿Cómo y por qué los atacantes usan proxies?. 2.3.2 Tipos de proxies. 2.3.3 Detección del uso de proxies. 2.3 Principales Técnicas utilizadas por los ciberdelincuentes. 2.3.1 Ingeniería social. 2.3.2 Phishing 2.3.3Pop ups. 2.3.4Email bombing and spamming. 2.3.5Keyloggers. 2.3.6 Man, in the middle. 2.3.7 Malware. 2.3.8 Nuevas técnicas utilizadas 2.4 Evaluación y gestión de la vulnerabilidad. 2.5 Caso de estudio
3	Pruebas De Penetración E Informática Forense.	3.1 Tipos de pruebas de penetración. 3.1.1 Prueba de penetración. 3.1.2 Pruebas de penetración utilizando aplicaciones web. 3.1.3 Prueba de penetración de red. 3.1.4Pruebas de penetración a móviles. 3.1.6 Pruebas de penetración usando ingeniería social. 3.1.7 Pruebas de penetración física. 3.2 Definición de informática forense. 3.3 Objetivos del análisis forense. 3.4Razones que desencadenan un análisis forense. 3.5 Roles representados en un caso forense. 3.5.1 Testigo.

		3.5.2 Cómplice. 3.5.3 Victima. 3.5.4 El Guardián. 3.5.5 Investigador Forense. 3.6 Casos de Alto Perfil 3.7 Metodología de un caso Forense. 3.8Evaluación del Caso: Detección, Identificación del evento, crimen. 3.8.1Preservación de la evidencia: Cadena de Custodia. 3.8.2Sanitizacion y preparación de dispositivos para colectar la evidencia. 3.8.3Recolección: Recuperación de los datos, Colección de la evidencia. 3.8.4Evaluación: Rastreando, filtrando, Extrayendo datos ocultos. 3.8.5Análisis de la información. 3.8.6Presentación de resultados. 3.9 Caso práctico.
4	Proyecto de Asignatura: Presentación y Defensa de Proyecto de Gestión Informática para Negocios.	5.1 Proyecto de Seguridad Lógica. 5.2. Proyecto de repositorio de datos. 5.3. Proyecto de visualización.

7. Actividades de aprendizaje de los temas

Conceptos Generales de la Seguridad Digital.	
Competencias	**Actividades de aprendizaje**
Específica(s): Analiza y comprende los conceptos básicos sobre Seguridad Digital en un ambiente lógico y físico, integrando medidas de aseguramiento de los canales lógicos por los cuales viajan los datos. Competencias instrumentales. • Capacidad de organizar y planificar. • Conocimientos generales básicos. • Toma de Decisiones. • Conocimientos básicos de la carrera. • Conocimiento en una segunda lengua. • Habilidades básicas de manejo de la computadora. • Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas. Solución de problemas. • Habilidades en el estudio y manejo de las TI emergentes Competencias Interpersonales. • Trabajo en equipo. • Capacidad de crítica y autocritica. • Capacidad de trabajar en equipo interdisciplinario. • Capacidad de comunicar con profesionales de otras áreas. • Capacidad para actuar en nuevas situaciones. • Compromiso ético. • Capacidad de administrar, organizar, planificar y liderar.	• Analizar los conceptos generales de Seguridad Digital. • Investigar la diferencia entre seguridad física y lógica. • Instalar y configurar diferentes sistemas operativos vulnerables proporcionados por la página de Pentester Lab. • Identificar los principales servicios de seguridad, clasificarlos según su grado de importancia y discutir su impacto de uso en las organizaciones. • Investigar las políticas vigentes aplicadas a la ciberseguridad en México. • Investigar las políticas vigentes aplicadas a la ciberseguridad en el ámbito internacional. • Investigar un caso de Estudio aplicados a los conceptos vistos en clases y exponerlo con el grupo. • Instalar y configurar herramientas de seguridad basadas en software libre y software licenciado, que permitan el aseguramiento lógico de los datos de un sistema informático. • Analizar y comparar los conceptos de Hacking Ético y Cracking. • Instalar y evaluar distintas herramientas de seguridad en el área de funciones Hash. • Realizar talleres a través de los casos prácticos, y presentar conclusiones al docente.

Competencias Sistémicas. • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Habilidad de trabajar de forma autónoma. • Diseño y gestión de proyectos.	
Vulnerabilidades Cibernéticas e Impactos.	
Competencias	**Actividades de aprendizaje**
Específica(s): Identifica los diferentes tipos de vulnerabilidades existentes en diversos sistemas operativos, realizando prácticas que permitan la clasificación de los distintos ataques utilizados y el nivel de riesgo que conlleva cada uno de ellos. Competencias instrumentales. • Capacidad de organizar y planificar. • Conocimientos generales básicos. • Toma de Decisiones. • Conocimientos básicos de la carrera. • Conocimiento en una segunda lengua. • Habilidades básicas de manejo de la computadora. • Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas. Solución de problemas. • Habilidades en el estudio y manejo de las TI emergentes Competencias Interpersonales. • Trabajo en equipo. • Capacidad de crítica y autocritica. • Capacidad de trabajar en equipo interdisciplinario.	• Investigar al menos 2 ataques que hayan sido gestados en el año que se cursa la materia y exponerlo en grupo. • Elaborar un cuadro informativo acerca de los tipos de vulnerabilidades cibernéticas detectadas en sistemas operativos libres y de licencia. • Realizar prácticas con sistemas operativos virtualizados en donde se puedan explotar diversas vulnerabilidades que permitan el análisis y documentación de las herramientas que se usan durante un ataque. • Elaborar un cuadro sinóptico donde se describan las principales técnicas antiforense que complican la investigación durante un caso forense digital informático. • Investigar un caso de Estudio aplicado a los conceptos vistos en clases y exponerlo con el grupo. • Realizar prácticas en donde se repliquen de manera ética las diversas técnicas que utilizan los ciberdelincuentes para gestar diversos ataques y de esta manera, crear contramedidas para evitar que en los sistemas se vean afectados por tales ataques.

• Capacidad de comunicar con profesionales de otras áreas. • Capacidad para actuar en nuevas situaciones. • Compromiso ético. • Capacidad de administrar, organizar, planificar y liderar. Competencias Sistémicas. • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Habilidad de trabajar de forma autónoma. • Diseño y gestión de proyectos.	• Realizar talleres en clase a través de los casos prácticos, y presentar conclusiones al docente. • Presentar contramedidas que permitan el aseguramiento del sistema operativo y protejan la integridad de los activos lógicos.
Pruebas de Penetración e Informática Forense.	
Competencias	**Actividades de aprendizaje**
Específica(s): Conoce, estudia y aplica las metodologías vigentes para el levantamiento de evidencias digitales, en casos forenses computacionales. Competencias instrumentales. • Capacidad de organizar y planificar. • Conocimientos generales básicos. • Toma de Decisiones. • Conocimientos básicos de la carrera. • Conocimiento en una segunda lengua. • Habilidades básicas de manejo de la computadora. • Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas. Solución de problemas.	• Investigar y definir ¿qué es? y ¿cómo se realiza una investigación forense digital? • Realizar un cuadro conceptual acerca de las principales actividades realizadas durante una investigación forense digital. • Instalar y configurar herramientas de software forense digital que permitan llevar una investigación de forma ordenada y detallas de los hechos encontrados durante la búsqueda de evidencia. • Investigar las metodologías aplicables en México para el desarrollo de una investigación forense digital, y posibles formas de evitar el problema investigado. • Realizar talleres a través de los casos prácticos, donde realicen levantamiento de información de casos forenses aplicables al tema.

• Habilidades en el estudio y manejo de las TI emergentes Competencias Interpersonales. • Trabajo en equipo. • Capacidad de crítica y autocritica. • Capacidad de trabajar en equipo interdisciplinario. • Capacidad de comunicar con profesionales de otras áreas. • Capacidad para actuar en nuevas situaciones. • Compromiso ético. • Capacidad de administrar, organizar, planificar y liderar. Competencias Sistémicas. • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Habilidad de trabajar de forma autónoma. • Diseño y gestión de proyectos.	• Realizar practicas de sanitización de dispositivos de almacenamiento externo que permitan al alumno conocer métodos de borrado seguro de los datos. • Realizar practicas de etiquetado de evidencias utilizando hashes para el correcto traslado de evidencias digitales y físicas a un laboratorio forense. • Elaboración de informes de los análisis encontrados durante la investigación forense digital. • Exposición de los diversas practicas realizadas durante el estudio del tema.
Proyecto Integrador: **Presentación y Defensa de Proyecto de Gestión Informática para Negocios.**	
Competencias	**Actividades de aprendizaje**
Específica: Elabora un proyecto de gestión informática aplicado a los negocios en las organizaciones. Competencias instrumentales. • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Conocimientos generales básicos. • Conocimientos básicos de la carrera. • Comunicación oral y escrita en su propia lengua.	• Presentar mediante exposición un proyecto de repositorio de datos alimentado de distintas fuentes aplicado a una organización. • Presentar mediante exposición un proyecto que tablero de control para la visualización de indicadores sobre una organización. • Presentar mediante exposición un proyecto de seguridad lógica de vulnerabilidades y pruebas de penetración que garanticen los

• Habilidades básicas de manejo de la computadora. • Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas). • Solución de problemas. • Toma de decisiones. Competencias interpersonales. • Capacidad crítica y autocrítica. • Habilidades interpersonales. • Capacidad de trabajar en equipo interdisciplinario. • Capacidad de comunicarse con profesionales de otras áreas. • Habilidad para trabajar en un ambiente laboral. Competencias sistémicas. • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. • Capacidad de adaptarse a nuevas situaciones. • Capacidad de generar nuevas ideas (creatividad). • Habilidad para trabajar en forma autónoma. • Capacidad para diseñar y gestionar proyectos. • Iniciativa y espíritu emprendedor. • Preocupación por la calidad. Búsqueda del logro.	niveles de seguridad de los activos lógicos de una organización.

8. Práctica(s)

• Instalar y configurar máquinas virtuales que permitirán simular diferentes entornos de trabajo, donde se pueden gestar los ataques. • Instalar sistemas operativos Linux enfocados al pentesting dentro de las maquinas virtuales y probar las herramientas que vengan incluidos con el paquete de software.

- Descargar y estudiar diversos casos de estudio de ataques informáticos que permitan reforzar conceptos teóricos vistos en clase.
- Instalar y configurar diferentes programas criptográficos que permitan analizar el nivel de seguridad que se maneja en un canal de comunicaciones.
- Realizar la elaboración de un modelo de encriptamiento para posteriormente llevarlo a la práctica.
- Realizar prácticas de análisis forense digital, utilizando metodologías aplicables para el levantamiento de información en México.
- Realizar practicas de Sanitización de medios de almacenamiento que servirán para el traslado de evidencia a el laboratorio forense.
- Instalación de software que permita al alumno llevar a cabo la cadena de custodia de manera ordenada en casos forenses digitales.
- Realizar una prueba de detección de vulnerabilidades a algún equipo informático del laboratorio.
- Realizar pruebas de penetración utilizando herramientas libres que permitan determinar los niveles de riesgo existentes a los sistemas que están siendo auditados.
- Realizar una auditoría de red para identificar vulnerabilidades existentes en los equipos de una LAN, WAN.
- 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.
- Seleccionar una organización o empresa del entorno para realizar en ella la implementación de un Plan de Seguridad. presentarse como proyecto integrador buscando reconocer las vulnerabilidades de la organización y cómo prevenir y minimizar los riesgos.
- Presentar y defender a través de exposición la propuesta de proyecto de gestión informática para negocios planteada.

9. Proyecto de asignatura

El objetivo del proyecto integrador es que el estudiante demuestre mediante la presentación de un proyecto único el alcance de las competencias generales de las 3 materias del noveno semestre que integran la especialidad de Gestión Informática para Negocios.

- **Fundamentación:** El estudiante deberá presentar un proyecto que contenga la información conceptual sobre la construcción de un repositorio, así como de las distintas fuentes de datos que lo integran y permitan la visualización de los mismos en graficas que sirvan para la toma de decisiones o muestren el análisis situacional de la organización, implementando medidas de aseguramiento al sistema que ayuden a evitar las principales vulnerabilidades que se puedan gestar tanto en sus sistemas operativos libres como en privados, agregando un reporte de las pruebas de penetración que se realizaron previamente y que ayuden a garantizar la integridad de los activos lógicos con los cuales se estará interactuando.

- **Planeación:** El proyecto deberá ser presentado por los estudiantes de manera individual al conjunto de profesores que imparten las asignaturas de la especialidad en noveno semestre a partir de la semana 15. La estructura de la presentación de proyecto será la misma para todos los alumnos.

- **Ejecución:** Los estudiantes deberán mostrar a través de la presentación de su proyecto el alcance de las competencias establecidas en las asignaturas de la especialidad en noveno semestre. Deberán basar la presentación de su proyecto de acuerdo con los requerimientos establecidos por la rúbrica previamente establecida,

- **Evaluación:** La evaluación será integral, es decir los profesores involucrados emitirán su evaluación mediante un instrumento único y preestablecido “rúbrica de evaluación del proyecto”. La evaluación hecha por los profesores generará retroalimentación a los estudiantes de manera inmediata con la finalidad de generar un tipo de “evaluación para la mejora continua”.

10. Evaluación por competencias

Las técnicas, instrumentos y herramientas sugeridas para constatar los desempeños académicos de las actividades de aprendizaje, la evaluación debe de ser continua y cotidiana por lo que debe considerar el desempeño en cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Instalación de Software.
- Cuadros conceptuales.
- Exposición de conceptos.
- Exposición de prácticas realizadas.
- Investigación de conceptos.
- Rubrica.
- Proyecto Integrador.
- Prácticas de forense digital.
- Talleres prácticos.

11. Fuentes de información

C. Joseph Touhill, G. J. (s.f.). Cybersecurity for Executives: A Practical Guide. Wiley-AIChE.

Carol C. Woody, N. R. (2016). Cyber Security Engineering: A Practical Approach for Systems and Software Assurance. Addison-Wesley Professional.

David O. Manz, T. W. (2017). Research Methods for Cyber Security. Syngress.

DeFranco, J. F. (2013). What Every Engineer Should Know About Cyber Security and Digital Forensics. CRC Press.

Donald Short, P. C. (2018). Cybersecurity Essentials. Sybex.

Dykstra, J. (2015). Essential Cybersecurity Science. O'Reilly Media, Inc.

Erdal Ozkaya, Y. D. (2019). Cybersecurity – Attack and Defense Strategies - Second Edition. Packt Publishing.

J. David Irwin, C.-H. W. (2016). Introduction to Computer Networks and Cybersecurity. CRC Press.

Jack J. Domet, T. J. (s.f.). A Leader's Guide to Cybersecurity. Harvard Business Review Press.

Joseph Weiss, J. S. (2012). Cyber Security Policy Guidebook. Wiley.

Raj Samani, E. D. (2013). Applied Cyber Security and the Smart Grid. Syngress.

Roman V. Yampolskiy, B. G. (2019). Cybersecurity. Harvard Business Review Press.

Sari Greene, O. S. (2018). Developing Cybersecurity Programs and Policies, Third Edition. Pearson IT Certification. Obtenido de https://learning.oreilly.com/library/view/developing-cybersecurity-programs/9780134858623/

Sari Greene, O. S. (2018). Developing Cybersecurity Programs and Policies, Third Edition. Pearson IT Certification.

Sathnur, A. (2019). The Business of Cybersecurity. Business Expert Press.

Stallings, W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards, First Edition. Addison-Wesley Professional.

Sutton, D. (2017). Cyber Security: A practitioner's guide. BCS Learning & Development Limited.

Tanner, N. H. (2019). Cybersecurity Blue Team Toolkit. Wiley.

Vacca, J. R. (2013). Cyber Security and IT Infrastructure Protection. Syngress.

William Rothwell, D. K. (2018). Linux Essentials for Cybersecurity, First Edition. Pearson IT Certification. Obtenido de https://learning.oreilly.com/library/view/linux-essentials-for/9780134853017/

William Rothwell, D. K. (2018). Linux Essentials for Cybersecurity, First Edition. Pearson IT Certification.

Wright, C. (2019). How Cyber Security Can Protect Your Business - A guide for all stakeholders. IT Governance Publishing.