1.- DATOS DE LA ASIGNATURA

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

2.- PRESENTACIÓN

Caracterización de la asignatura.

Esta asignatura aporta al perfil del Ingeniero Informático las capacidades de aplicar conocimientos científicos y tecnológicos en la solución de problemas en el área informática con un enfoque interdisciplinario; de seleccionar y utilizar de manera óptima técnicas y herramientas computacionales actuales y emergentes; y la aplicación de normas, marcos de referencia y estándares de calidad y seguridad vigentes en el ámbito del desarrollo y gestión de tecnologías y sistemas de información.

Para conformarla, se ha hecho un análisis de las características que son necesarias conocer para implementar diferentes herramientas y técnicas de seguridad basados, sobre todo, en las características propias que tiene Internet con el fin de mantener la integridad de la información en sistemas de redes de computadoras.

Esta materia se ha incluido en el V semestre, debido a que necesita, para su completa comprensión, del manejo de conceptos de matemáticas tales como álgebra lineal, probabilidad, estadística, etc. A su vez, servirá como base y complemento para otras materias del área de redes, en el sentido de los aspectos que ésta abarcará, puesto que, si bien las demás abarcarán aspectos relacionados con seguridad, no contendrán la base lógica que es lo que proporciona esta materia, con el fin de entender el cómo y el por qué son necesarias las tecnologías que se describirán y se usarán después.

Intención didáctica.

Se organiza el temario, en seis unidades, agrupando, básicamente, los contenidos conceptuales de la asignatura en las unidades uno y tres, y aunque las demás son más aplicadas, incluyen una pequeña parte de conceptos teóricos necesarios para su correcto entendimiento, procurando que en cada una de estas últimas centrarse mucho en la parte de la aplicación de los conceptos.

En la primera unidad, 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.

---

[1] *Sistema de Asignación y Transferencia de Créditos Académicos*

En la segunda unidad se abordan los algoritmos criptográficos desarrollados a lo largo de la historia, empezando desde la antigüedad, pasando por los cifradores del siglo XIX, hasta llegar a los criptosistemas conocidos como clásicos y algunas máquinas de cifrar desarrolladas en el siglo XX, así como un análisis de la importancia que tiene el conocimiento de la estadística del lenguaje para el análisis y posible rompimiento de los algoritmos criptográficos.

La tercera unidad es otra unidad básicamente conceptual, más que aplicada, (salvo al final), pero que permitirá tener una idea de la aplicación y complejidad en ésta que tienen los certificados y las firmas digitales. E inicia esta unidad con el concepto de la distribución de claves, de a qué se refiere la certificación, los componentes de una PKI (infraestructura de clave pública) y las diferentes arquitecturas PKI actualmente en uso, las características y diferencias entre las políticas y las prácticas de certificación, la comprensión de lo que implica la gestión de una PKI, así como el conocimiento de los estándares y protocolos de certificación vigentes. Al final, se sugiere una práctica integradora con un generador de certificados gratuito, en línea y libre, como puede ser OpenCA, que sirva de referencia didáctica y en la cual se puedan ver ejemplificados los conceptos manejados a lo largo de la unidad.

La siguiente unidad se refiere a un estudio introductorio a la seguridad en redes, considerando aspectos de la seguridad en las comunicaciones, analizando las debilidades de los protocolos TCP/IP, revisando los estándares existentes para la seguridad en redes, así como haciendo un estudio sobre la seguridad en redes inalámbricas, tan de moda actualmente. Cabe recordar que estos aspectos serán tratados más a profundidad en materias posteriores.

La unidad 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 algunos aspectos introductorios a la vigilancia de los sistemas de información, iniciando con la definición de vigilancia, la anatomía de un ataque (haciendo referencia y ejemplificando los conceptos vistos en las primeras unidades), a qué se refiere el escaneo, la identificación de vulnerabilidades, algunas posibles actividades de infiltración, la consolidación y terminará con una referencia más a fondo de la defensa perimetral y su importancia.

El enfoque sugerido para la materia requiere que las actividades prácticas promuevan el desarrollo de habilidades para la experimentación, tales como: identificación, manejo y control de herramientas de desarrollo de software, lenguajes de programación, 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 sólo guiar a sus alumnos para que ellos hagan la elección de los elementos

a programar y la manera en que los tratarán. 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 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 alumno 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.

Es necesario que el profesor ponga atención y cuidado en estos aspectos en el desarrollo de las actividades de aprendizaje de esta asignatura.

3.- COMPETENCIAS A DESARROLLAR

Competencias específicas:	**Competencias genéricas:**	
▪ Hacer uso de las herramientas de software para contribuir a mejorar los niveles de seguridad informática en una organización.	*Competencias instrumentales* • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Conocimientos básicos de la carrera. • Comunicación oral y escrita. • Habilidades de manejo de la computadora. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. *Competencias interpersonales* • Capacidad crítica y autocrítica. • Trabajo en equipo. • Habilidades interpersonales. *Competencias sistémicas* • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. • Capacidad de generar nuevas ideas (creatividad). • Habilidad para trabajar en forma autónoma. • Búsqueda del logro.	

4.- HISTORIA 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, 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 Diseño e Innovación Curricular para el Desarrollo y Formación de Competencias Profesionales de la Carrera de Ingeniería Informática.
Desarrollo de Programas en Competencias Profesionales por los Institutos Tecnológicos del 12 de octubre de 2009 al 19 de febrero de 2010.	Academias de Ingeniería Informática de los Institutos Tecnológicos de: Superior del Occidente del Estado de Hidalgo y Superior de Valladolid.	Elaboración del programa de estudio propuesto en la Reunión Nacional de Diseño Curricular de la Carrera de Ingeniería Informática.
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 la Carrera de Ingeniería Informática.

5.- OBJETIVO GENERAL DEL CURSO

Hacer uso de las herramientas de software para contribuir a mejorar los niveles de seguridad informática en una organización.

6.- COMPETENCIAS PREVIAS

- Conocimiento en el manejo y funcionalidad de los sistemas de información (bases de datos), redes de computadores, software base (sistemas operativos, lenguajes de programación).

7.- TEMARIO

Unidad	Temas	Subtemas
1.	Introducción a la seguridad informática	1.1. El valor de la información. 1.2. Definición y tipos de seguridad informática. 1.3. Objetivos de la seguridad informática. 1.4. Posibles riesgos. 1.5. Técnicas de aseguramiento del sistema.
2.	Criptografía clásica: Un primer acercamiento	2.1. En la antigüedad. 2.2. Cifradores del siglo XIX. 2.3. Criptosistemas clásicos. 2.4. Máquinas de cifrar (siglo XX) y estadística del lenguaje.
3.	Certificados y firmas digitales	3.1. Distribución de claves. 3.2. Certificación. 3.3. Componentes de una PKI. 3.4. Arquitecturas PKI. 3.5. Políticas y prácticas de certificación. 3.6. Gestión de una PKI. 3.7. Estándares y protocolos de certificación. 3.8. Ejemplo de un protocolo de seguridad: HTTPS. 3.9. SSL, TSL, SSH. 3.10. Prueba con un generador de certificados gratuito, libre y en línea.
4.	Seguridad en redes	4.1. Aspectos de seguridad en las comunicaciones. 4.2. Debilidades de los protocolos TCP/IP. 4.2.1. Transmisión de paquetes y promiscuidad. 4.2.2. Redes locales (VLAN) y amplias (VPN). 4.2.3. Domicilios IP. 4.2.4. Vigilancia de paquetes. 4.3. Estándares para la seguridad en redes. 4.4. Vulnerabilidad de los protocolos inalámbricos WEP, WPA, WPA2.
5.	Firewalls como herramientas de seguridad	5.1. Tipos de firewall: de software y de hardware. 5.1.1. Firewall de capas inferiores.

		5.1.2. Firewall de capa de aplicación. 5.1.3. Firewall personal. 5.2. Ventajas de un firewall. 5.3. Limitaciones de un firewall. 5.4. Políticas del firewall. 5.5. Enlaces externos.
6.	Vigilancia de los sistemas de información	6.1. 6.1 Definición de vigilancia. 6.2. Anatomía de un ataque. 6.2.1. Identificación de objetivos. 6.2.2. Reconocimiento inicial. 6.2.3. Técnicas de recopilación de información y análisis forense. 6.3. Escaneos. 6.3.1. Identificación y ataques a puertos TCP/UDP. 6.3.2. Identificación y ataques a servicios. 6.4. Identificación de vulnerabilidades. 6.4.1. Técnicas manuales. 6.4.2. Técnicas automáticas. 6.5. Actividades de infiltración. 6.5.1. Sistema operativo. 6.5.2. Aplicaciones. 6.5.3. Bases de datos. 6.6. Consolidación. 6.7. Defensa perimetral. 6.7.1. Creación de una DMZ. 6.7.2. Antivirus. 6.7.3. Nat. 6.7.4. Proxy

8.- SUGERENCIAS DIDÁCTICAS

El docente debe:

Ser conocedor de la disciplina que está bajo su responsabilidad, conocer su origen y desarrollo histórico para considerar este conocimiento al abordar los temas. Desarrollar la capacidad para coordinar y trabajar en equipo; orientar el trabajo del estudiante y potenciar en él la autonomía, el trabajo cooperativo y la toma de decisiones. Mostrar flexibilidad en el seguimiento del proceso formativo y propiciar la interacción entre los estudiantes. Tomar en cuenta el conocimiento de los estudiantes como punto de partida y como obstáculo para la construcción de nuevos conocimientos.

- Propiciar actividades de metacognición. Ante la ejecución de una actividad, señalar o identificar el tipo de proceso intelectual que se realizó: una identificación de patrones, un análisis, una síntesis, la creación de un heurístico, etc. Al principio lo hará el profesor, luego será el alumno quien lo identifique. Ejemplos: reconocer los aspectos matemáticos involucrados en el proceso de encriptación: reconocimiento de patrones, elaboración de una regla o método de encriptación o desencriptación a partir de una serie de observaciones: síntesis.
- Propiciar actividades de búsqueda, selección y análisis de información en distintas fuentes. Ejemplo: buscar y contrastar definiciones de seguridad en internet y redes, en general, identificando puntos de coincidencia entre unas y otras definiciones e identificar sus características y aplicaciones en situaciones concretas.
- Fomentar actividades grupales que propicien la comunicación, el intercambio argumentado de ideas, la reflexión, la integración y la colaboración de y entre los estudiantes. Ejemplo: al socializar los resultados de las investigaciones y las experiencias prácticas solicitadas como trabajo extra clase.
- Observar y analizar fenómenos y problemáticas propias del campo ocupacional. Ejemplos: el proyecto que se realizará en la unidad 2 y varias de las actividades sugeridas para las unidades 2, 5 y 6.
- Relacionar los contenidos de esta asignatura con las demás del plan de estudios a las que ésta da soporte para desarrollar una visión interdisciplinaria en el estudiante. Ejemplos: identificar las tipologías de ataques a las redes y la manera de protegerlos a través de los elementos de red, las capas del modelo OSI a la que está dirigido, etc.
- Propiciar el desarrollo de capacidades intelectuales relacionadas con la lectura, la escritura y la expresión oral. Ejemplos: trabajar las actividades prácticas a través de guías escritas, redactar reportes e informes de las actividades de experimentación, exponer al grupo las conclusiones obtenidas durante las observaciones.
- Facilitar el contacto directo con materiales e instrumentos, al llevar al cabo actividades prácticas, para contribuir a la formación de las competencias para el trabajo experimental como: identificación, manejo y control de equipos y datos relevantes, planteamiento de hipótesis, trabajo en equipo.
- Propiciar el desarrollo de actividades intelectuales de inducción-deducción y análisis-síntesis, que encaminen hacia la investigación.
- Desarrollar actividades de aprendizaje que propicien la aplicación de los conceptos, modelos y metodologías que se van aprendiendo en el desarrollo de la asignatura.
- Proponer problemas que permitan al estudiante la integración de contenidos de la asignatura y entre distintas asignaturas, para su análisis y solución.
- Relacionar los contenidos de la asignatura con el cuidado del medio ambiente; así como con las prácticas de una agricultura sustentable.
- Cuando los temas lo requieran, utilizar medios audiovisuales para una mejor comprensión del estudiante.

- Propiciar el uso de las nuevas tecnologías en el desarrollo de la asignatura (procesador de texto, hoja de cálculo, base de datos, graficador, Internet, sistemas de gestión de contenidos, etc.).

9.- SUGERENCIAS DE EVALUACIÓN

La evaluación debe ser continua y formativa por lo que se debe considerar el desempeño en cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Presentación de reportes de búsqueda de información en fuentes bibliográficas o digitales de reconocido valor, las cuales deben ir indicadas por el instructor.
- Participación en actividades para demostrar el entendimiento y comprensión de los conocimientos adquiridos a través de las investigaciones anteriores, tales como la elaboración de mesas panel, etc.
- Elaboración de proyectos de aplicación donde se incluyan e integren los algoritmos vistos en clase y programados fuera de ellos.
- Entrega de los algoritmos programados.
- Examen escrito donde se pueda comprobar el manejo de conocimientos teóricos y declarativos.
- Reportes escritos de las observaciones hechas durante las actividades, así como de las conclusiones obtenidas de dichas observaciones.
- Elaboración de manuales de instalación y configuración de las diferentes tecnologías abarcadas en el presente programa.

10.- UNIDADES DE APRENDIZAJE

Unidad 1: Introducción

Competencia específica a desarrollar	*Actividades de Aprendizaje*
Reconocer la importancia y complejidad que implica el concepto de seguridad en el ámbito de la informática y las diferentes áreas en las cuales está inmersa.	• Elaborar por medio de una lluvia de ideas el significado de seguridad en informática. • Investigar y discutir cuál es el valor real que se le da a la información en nuestros días. • Investigar la definición de seguridad en informática en fuentes no confiables y fuentes bien respaldadas. Comparar ambos resultados e identificar diferencias y similitudes. • Realizar un mapa conceptual con la definición de seguridad informática. • Investigar los objetivos que persigue la seguridad en el ámbito informático. • Esquematizar estos objetivos en mapas mentales, conceptuales o cuadros sinópticos. • Investigar los posibles riesgos a los que se enfrentan las empresas al no tomar en cuenta aspectos de seguridad informática. • Discutir en una mesa panel estos posibles riesgos. • Redactar las conclusiones de la mesa panel. • Investigar y categorizar las diferentes técnicas existentes para el aseguramiento de un sistema. • Discutir estas técnicas, desde el punto de

	vista de sus características, ventajas y desventajas, fortalezas y debilidades. • Investigar posibles escenarios de uso de estas técnicas y ejemplos de aplicación para el cumplimiento de los objetivos de la seguridad en informática.

Unidad 2: Criptografía clásica: Un primer acercamiento

Competencia específica a desarrollar	*Actividades de Aprendizaje*
Implementar algoritmos de criptografía clásica con el fin de proteger la información que se transmite a través de una aplicación.	• Investigar los algoritmos utilizados para "esconder" la información y que ésta no sea legible de manera directa por cualquier persona, desde la antigüedad, tales como la escítala, y el algoritmo de César, entre otros. • Investigar los algoritmos desarrollados durante el siglo XIX, así como también una breve biografía de sus creadores. • Investigar el concepto de criptografía clásica y la clasificación de este tipo de criptosistemas. • Elaborar mapas conceptuales y cuadros sinópticos con la información recabada. • Intercambiar y discutir con los demás compañeros sus hallazgos • Llevar al cabo en el salón la implementación manual de estos algoritmos. • Implementar en un lenguaje de programación estos algoritmos. • Investigar las características, creadores y funcionamiento de algunas máquinas para cifrar desarrolladas en el siglo XX, tales como la máquina Enigma. • Crear carteles, tipo congresos, en los cuales se presente esta información. • Entender el concepto de estadística del lenguaje y su aplicación como primer acercamiento al criptoanálisis.

Unidad 3: Certificados y firmas digitales

Competencia específica a desarrollar	*Actividades de Aprendizaje*
Crear un certificado digital, con el fin de proteger la información de una entidad al momento de hacer transacciones en la web de una manera segura.	• Investigar el funcionamiento de la distribución de claves, tanto en métodos simétricos (haciendo referencia a los algoritmos vistos en la unidad anterior), como asimétricos. • Por lluvia de ideas, derivar el concepto de

	certificado y extrapolarlo al ámbito digital. • Investigar el concepto de certificado digital y elaborar con ello un mapa conceptual, el cual intercambiará con sus demás compañeros. • Investigar el proceso de certificación, identificando las partes involucradas, sus funciones, los requerimientos, etc. • Elaborar un diagrama en el que se reflejen todos estos pasos o llevar al cabo un sociodrama en el que se refleje este procedimiento. • Identificar los componentes de una infraestructura de clave pública, sus funciones y sus responsabilidades. • Investigar las diferentes arquitecturas de una PKI, haciendo una comparación entre ellas, y analizando sus ventajas y desventajas, fortalezas y debilidades, así como el establecimiento de posibles escenarios de uso. • Investigar los conceptos de prácticas y políticas de certificación, identificando su diferencia. • Investigar el proceso de gestión de una PKI, identificando las partes involucradas, sus funciones y sus responsabilidades. • Elaborar un diagrama en el cual se describa este proceso. • Investigar y ejemplificar los estándares y protocolos existentes para el proceso de certificación, sus características, si están vigentes y en uso actualmente o no, funcionamiento, etc. • Realizar una práctica de creación de certificado utilizando una herramienta gratuita y en línea, como es OpenCA.

Unidad 4: Seguridad en redes

Competencia específica a desarrollar	*Actividades de Aprendizaje*
Crear conciencia y proteger la información de una empresa a través del reconocimiento de las debilidades inherentes de las tecnologías aplicadas a una red de computadoras.	• Investigar y discutir en un debate los aspectos de seguridad generales de las comunicaciones. • Analizar el funcionamiento del protocolo TCP/IP. • Conocer como se da el control de acceso a los medios. • Investigar, distinguir e identificar las

	debilidades inherentes a los protocolos TCP/IP y demás relacionados con las redes, haciendo una comparación entre ellos. • Investigar los diferentes estándares existentes en el ámbito de la seguridad en redes de computadoras, analizando sus características, ventajas y desventajas y diseñando escenarios de aplicación. • Traspolar los conocimientos adquiridos anteriormente, para la seguridad en redes inalámbricas, haciendo énfasis en los protocolos WEP, WAP y WPA2. Haciendo una comparación entre estas redes y las basadas en cables. • Conocer y aplicar el funcionamiento de los protocolos que existen en redes y redes inalámbricas y sus diferencias. • Analizar de las diversas vulnerabilidades que pueden presentar las redes wireless.

Unidad 5: Firewalls como herramienta de seguridad

Competencia específica a desarrollar	*Actividades de Aprendizaje*
Implementar un firewall como método de protección de la información que se recibe de un medio externo y que se transmite hacia afuera de una red de computadoras.	• Investigar qué es un firewall, para qué sirve, sus características y clasificación. • Plantear escenarios de aplicación de un firewall. • Investigar productos comerciales y gratuitos, tanto de firewalls de software como de hardware. • 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 con IPcop de Linux.

Unidad 6: Vigilancia de los sistemas de información

Competencia específica a desarrollar	*Actividades de Aprendizaje*
Llevar al cabo una vigilancia e implementar medidas de seguridad efectivas de la información que circula	• Realizar una lluvia de ideas acerca del significado del concepto de vigilancia,

a través de una red.	extrapolándolo, posteriormente, al ámbito informático. • Investigar los tipos de ataques que se pueden presentar aun sistema de información a través de una red de datos, haciendo una comparación con los tipos de ataques vistos en unidades anteriores, principalmente, en la parte de criptografía. Identificar sus características, las vulnerabilidades en los sistemas a los cuales atacan, etc. • Investigar cuál es el concepto de escaneo y cuáles tipos hay, a qué va dirigido, de qué herramientas se valen, etc. • Investigar los diferentes métodos de infiltración que se pueden dar, a través de qué, utilizando cuáles herramientas, cómo funcionan dichas herramientas, etc. Presentar escenarios en los cuales estos ataques se den. • Especificar la manera en que la defensa, a nivel perimetral, protege a los sistemas de información de este tipo de ataques, escenificando o ejemplificando estas situaciones. • Instalar herramientas de monitoreo y análisis de tráfico de una red, explicando su funcionamiento y haciendo referencia a los diferentes tipos de ataques y las vulnerabilidades de las que se aprovecha. • Investigar el origen del concepto de zona desmilitarizada (DMZ, por sus siglas en inglés) y su aplicación al ámbito informático. • Creación de una DMZ utilizando herramientas gratuitas.

11.- FUENTES DE INFORMACIÓN

1. Aguirre, Jorge R. *"Aplicaciones Criptográficas."* Segunda edición. Junio, 1999. Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España. ISBN 83-87238-57-2.
2. Zimmermann, P. *"An Introduction to Cryptograpy".* Network Associates. 1999, available at: ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf.
3. Zimmermann, Philip R*. "Cryptography for the Internet."* Scientific American. October, 1998.
4. Diffie, Whitfield; Landau, Susan Eva. *"Privacy on the Line."* MIT Press. ISBN: 0262041677.
5. Biham, Eli; Shamir, Adi. *"Differential Cryptanalysis of the Data Encryption Standard."* Springer-Verlag. ISBN: 0-387-97930-1 A .
6. Kaufman, Charlie; Perlman, Radia; Spencer, Mike. *"Network Security: Private Communication in a Public World".* Prentice Hall. ISBN: 0-13-061466-1.
7. Schneier, Bruce. *"Applied Cryptography: Protocols, Algorithms, and Source Code in C."* John Wiley & Sons. ISBN: 0-471-12845-7.
8. Smith, Richard E. *"Internet Cryptography."* Addison-Wesley Pub Co. ISBN: 0201924803.
9. Cheswick, William R.; Bellovin, Steven M. *"Firewalls and Internet Security: Repelling the Wily Hacker."* Addison-Wesley Pub Co. ISBN: 0201633574.
10. Cano-Barrón, José E.; Martínez-Peláez, Rafael; Soriano, Miquel. *"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). Oct. 11 – 13, 2007. Koblenz, Alemania.
11. Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A. *"Handbook of applied cryptography"*. ISBN: 0-8493-8523-7. Oct., 1996.
12. Koblitz, Neal. *"A Course in Number Theory and Cryptography".* Springer-Verlag. ISBN: 0-387-94293-9.
13. Aguirre, Jorge R. "*Libro Electrónico de Seguridad Informática y Criptografía*". ISBN 84-86451-69-8 (2006); Depósito Legal M-10039-2003. Disponible en Internet en http://www.criptored.upm.es/guiateoria/gt_m001a.htm.
14. Lucena López, Manuel J. "*Criptografía y Seguridad en Computadores*". Cuarta Edición. Versión 0.7.8. 9 de octubre de 2007. *Criptografía y Seguridad en Computadores es un libro electrónico en castellano, publicado bajo licencia Creative Commons*.
15. Khan, David. "*The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet*". Revised and Updated. Scribner. 1996. ISBN: 0684831309.
16. Schneier, Bruce. "*Applied Cryptography*". Second Edition. John Wiley & Sons, 1996. ISBN 0-471-11709-9.
17. Singh, Simon. "*Los Códigos Secretos. El Arte y la Ciencia de la Criptografía desde el Antiguo Egipto a la Era de Internet*". Editoral Debate, 2000. ISBN: 84-8306-278-X.
18. Ángel Ángel, José de Jesús. *"Criptografía para Principiantes".* Obtenido en la red mundial el 5 de noviembre de 2002. 2000. http://www.criptored.upm.es/descarga/cripto_basica.zip.
19. Anónimo. *"Máxima Seguridad en Linux"*.Prentice Hall.

12.- PRÁCTICAS PROPUESTAS

- Instalación y administración de un sistema de cortafuegos:
- Firewall por hardware
- Firewalls por software
- Instalación de un servidor headless.
- Creación de un servidor web, asignación de IP pública con el fin de practicar y mostrar su vulnerabilidad si no es configurado de manera adecuada.
- Ejemplos con mínimo 2 sistemas operativos.
- Instalación de Soluciones de Antivirus Centralizadas.
- Creación de un Servidor Proxy en diversas plataformas
- Uso de herramientas de monitoreo de red.
- Uso de IPSEC.
- Elaboración manual de los algoritmos de encriptación, cuando sea posible, sobre todo para los algoritmos de la antigüedad.
- Programación de cada uno de los algoritmos criptográficos.
- Formulación de una política de seguridad.
- Instalación, configuración y administración de un Firewall con IPcop
- Instalación de un servidor Proxy con SQUID.
- Instalación de un servidor Proxy con ISA Server
- Instalación de una aplicación centralizada con Symantec o alguna solución de antivirus que posea.
- Instalación de un servidor de Directorio con Windows 2003.
- Instalación y pruebas de seguridad de una red inalámbrica.
- Instalación de un servidor WEB con Apache en Linux, IIS en Windows 2003.
- Instalación de herramientas bajo el modelo NSM.
- Formulación de un esquema de red segura con la implementación de todas las prácticas anteriores elaboradas.
- Llevar al cabo la elaboración de un certificado digital utilizando alguna herramienta gratuita y en línea, como puede ser OpenCA.
- Hacer una prueba con Aircrack.