1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad de la Infraestructura Tecnológica
Clave de la asignatura:	SCF-2002
SATCA[1]:	*3-2-5*
Carrera:	Ingeniería en Sistemas Computacionales

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta al perfil del ingeniero en sistemas computacionales la capacidad analítica para clasificar y usar diferentes métodos para implementar la seguridad de la Infraestructura Tecnológica. En esta asignatura se estudian técnicas criptográficas que son fundamentales para entender el cómo funciona la seguridad informática en la actualidad.

Para conformar esta materia, se ha hecho un análisis de las características que son necesarias conocer para implementar diferentes herramientas y técnicas de seguridad basados, en las particularidades propias de Internet, Firewalls y VPN's con el fin de mantener la integridad de la información en las tecnologías.

Esta materia es introductoria a los conceptos básicos de criptografía, también se explican herramientas matemáticas que son esenciales para comprender cómo funcionan los sistemas criptográficos. Se tratarán las numerosas aplicaciones del mundo cotidiano que utilizan la criptografía.

Así mismo, se abordan la seguridad de los dispositivos móviles e IoT en aspectos como el almacenamiento, transmisión de datos y periféricos o integrados de autenticación por radio frecuencia. También las consideraciones del uso de dispositivos propios y servicios de voz sobre Ip en las organizaciones.

Para finalizar se revisan las principales vulnerabilidades y ataques que afectan a las bases de datos, planteando además estrategias, buenas prácticas, e implementación de herramientas para minimizarlas.

Intención didáctica

El estudio de esta materia se divide en cuatro temas donde el estudiante desarrollará la capacidad de diseñar esquemas de seguridad perimetral, evaluar riesgos y vulnerabilidades de los sistemas de información utilizando técnicas de Hacking Ético y diseñar planes de gestión de la seguridad de informática basados en normas. Se utilizará equipamiento, herramientas de código abierto y estándares internacionales, para que el

[1] Sistema de Asignación y Transferencia de Créditos Académicos

estudiante pueda implementar los conocimientos adquiridos en su entorno laboral o personal.

En el primer tema se abordan aspectos introductorios al curso, así como definiciones y los tipos de seguridad informática, anatomía de ataques a las redes informáticas, funcionalidad de Firewalls, utilidad de VPNs y Servidores AAA. Al estudiar cada parte, se incluyen los conceptos involucrados con ella para hacer un tratamiento más significativo, oportuno e integrado de dichos conceptos, haciendo un énfasis muy especial en la utilidad que tendrá para más adelante, tanto del desarrollo de la asignatura como de la carrera en general.

En el segundo tema, se tratarán las consideraciones básicas de seguridad de dispositivos móviles e Iot con un enfoque dirigido al almacenamiento de datos en ellos. Del mismo modo se analizarán los sistemas de telecomunicaciones y medios de transmisión como lo es Bluetooth, Wifi y la Red GSM. Se evaluará la viabilidad de usar sistemas de autenticación por radio frecuencia como los son NFC y RFID. Con una práctica con lectores y tarjetas de desarrollo open source. Se comparan los pros y contras de uso de los dispositivos propios en las organizaciones y la telepresencia por medio de VoIP y las consideraciones de seguridad elementales para su uso.

En el tercer tema, se describen las aplicaciones fundamentales de la criptografía: cifrado y firma electrónica. Ambas aplicaciones son el núcleo del comercio electrónico y de cualquier transacción segura que se realice por Internet. También se introduce el concepto de certificado digital y su importancia para garantizar la seguridad, así como las aplicaciones que mayor beneficio obtienen de su utilización.

En el cuarto tema se analizan las vulnerabilidades de las bases de datos, así como las estrategias y buenas prácticas para minimizarlas. Además, se revisan los modelos de seguridad relativos a este tipo de sistemas. También se identifican las herramientas asociadas a la seguridad y las funciones de manejo de confiabilidad, privilegios, permisos, respaldo y recuperación.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México campus San Juan del Río. Junio del 2020.	Ing. Barrón Osornio José Gaspar M.I.S.D. Dorantes Hernández Luz María. Ing. Suárez Álvarez Nancy Mireya Ing. Valdes Arteaga Leonardo	Reunión de Academia Carrera de Ingeniería en Sistemas Computacionales para el diseño de Módulo de Especialidad y elaboración de programas de estudio.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Identificar las diferentes vulnerabilidades en los sistemas de información y seguridad perimetral evaluando servicios y mecanismos necesarios para implementar una estrategia en la seguridad de la infraestructura Tecnológica, de acuerdo a los requisitos de la organización.

5. Competencias previas

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

6. Temario

No.	Temas	Subtemas
1	Seguridad en la Infraestructura Tecnológica y perimetral	1. Introducción 2. Seguridad en infraestructura tecnológica 3. Seguridad perimetral 3.1 Definición y componentes del perímetro de seguridad 3.2. Anatomía de ataques a las redes informáticas 4. Importancia de la seguridad a nivel red 4.1. Firewalls. 4.2. Firewalls basados en software y en hardware (appliances) 5. VPNs

		6. Servidores
2	Seguridad en Dispositivos Móviles e IoT	2.1 Dispositivos móviles e IoT 2.1.1 Introducción 2.1.2 Tipos de Dispositivos 2.1.3 Almacenamiento móvil 2.1.4 Seguridad en almacenamiento para dispositivos móvil 2.2 Seguridad en Sistemas de Telecomunicaciones 2.2.1 Bluetooth 2.2.2 Wifi 2.2.4 GSM 2.2.5 NFC y RFID 2.3 Uso de dispositivos propios (BYOD) 2.3.1 VPN y Servicios en la Nube 2.4 Seguridad en Voz sobre IP
3	Criptografía	3.1. Introducción a la criptografía 3.2. Criptografía y criptoanálisis 3.3. Historia de la Criptografía 3.3.1 Criptografía clásica 3.3.2 Criptografía en la actualidad 3.4. Tipos de Criptografía 3.4.1 Criptografía simétrica 3.4.2 Criptografía asimétrica 3.5. El criptosistema RSA 3.6. Infraestructura de llave pública y privada 3.7. Códigos de autenticación de mensaje 3.8. Certificados digitales y autoridades certificadoras
4	Seguridad en Base de datos	4.1. Tipos de bases de datos 4.2. Seguridad en los lenguajes de manejadores. 4.3. Seguridad en base de datos 4.3.1. Modelos de seguridad 4.3.2. Confidencialidad 4.3.3. Herramientas para el análisis de vulnerabilidades en bases de datos 4.4. Funciones del Administrador de la base de datos.

7. Actividades de aprendizaje de los temas

1. Seguridad en la infraestructura tecnológica y perimetral

Competencias	Actividades de aprendizaje
Específica(s): Adquiere conocimientos básicos de seguridad efectivas de la información que circula a través de una red. Genéricas: ● Habilidad para buscar y analizar información proveniente de fuentes diversas. ● Solución de problemas. ● Toma de decisiones. ● Capacidad de aplicar los conocimientos en la práctica. ● Habilidades de investigación.	● Investigar concepto de seguridad perimetral. ● Investigar los componentes de perímetro de seguridad. ● Investigar tres ataques a redes. ● Investigar cómo identificar y prevenir de un ataque a la red. ● Exponer en clase la identificación y prevención de un ataque. ● Exponer en clase la importancia de la seguridad en las redes. ● Investigar que es Firewalls. ● Realizar tabla comparativa de los Firewalls para redes. ● Exponer en clase las ventajas de Firewalls por hardware. ● Exponer la importancia, tipos y ejemplos de VPNs. ● Instalación de una VPN. ● Investigar función e importancia de los Servidores AAA.
2. Seguridad en Dispositivos Móviles e IoT	
Competencias	Actividades de aprendizaje
Específica(s): Identifica los principales medios de almacenamiento y transmisión de dispositivos móviles e IoT, con el objetivo de brindarles seguridad. Genéricas: ● Capacidad de análisis y síntesis. ● Capacidad de trabajo en equipo ● Capacidad para tomar decisiones. ● Habilidades para buscar, procesar y analizar información procedente	● Realizar una infografía sobre la clasificación de los dispositivos móviles y sus características ● Realizar una infografía sobre los tipos de dispositivos de IoT y sus características. ● Investigar sobre las principales vulnerabilidades de los dispositivos móviles tanto a nivel de acceso como de su almacenamiento y realizar un reporte técnico.

de fuentes diversas	• Investigar sobre las principales vulnerabilidades de los dispositivos de Iot tanto a nivel de acceso como de su almacenamiento y realizar un reporte técnico. • Diseñar un dispositivo de seguridad con una lectora rfid y una laptop que permita conceder acceso o no a una persona. • Analizar algún sistema de voz sobre ip verificando sus características de seguridad y realizar un reporte.
3. Criptografía	
Competencias	Actividades de aprendizaje
Específica(s): Adquiere conocimientos sobre los fundamentos matemáticos que sustentan la criptografía y en particular aquellos requeridos en los contenidos de la asignatura. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de trabajo en equipo • Capacidad para tomar decisiones. • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas	• Conocer los aspectos básicos de la teoría de la información y de complejidad necesarios para definir cualidades en un buen cripto sistema. • Distinguir entre ataques a los algoritmos criptográficos • Enumerar distintos métodos de certificación digital y conocer sus estándares • Conocer los principales algoritmos de clave secreta y pública, sus especificaciones y algunos criterios de diseño. • Decidir sobre el uso y la aplicación de los algoritmos criptográficos más adecuados, en situaciones donde es necesario proteger la confidencialidad de la información y la privacidad en las comunicaciones.
4. Seguridad en Base de Datos	
Competencias	Actividades de aprendizaje

Específica(s): Gestiona herramientas y mecanismos de seguridad asociadas a la seguridad de base de datos. Genéricas: ● Habilidad para buscar y analizar información proveniente de fuentes diversas. ● Solución de problemas. ● Toma de decisiones. ● Capacidad de aplicar los conocimientos en la práctica. ● Habilidades de investigación	● Diseñar una tabla comparativa de las características principales de los diferentes tipos de base de datos. ● Realizar una investigación guiada sobre las mejores prácticas para acceso y manipulación de datos entre los diferentes lenguajes de los manejadores de base de datos. ● Diseñar un mapa conceptual de las funciones de seguridad externa e interna. ● Enlistar las funciones de manejo de confiabilidad, privilegios, permisos, respaldo y recuperación de acuerdo al manejador de base de datos. ● Comparar los modelos de seguridad e identificar el modelo más adecuado de acuerdo a los requerimientos y necesidades. ● Realizar ejemplos de ataque de SQL injection y proponer soluciones. ● Realizar una investigación guiada sobre las diferentes herramientas asociadas a la seguridad de base de datos. ● Realizar un check list de las acciones a realizar por parte del administrador para reducir las vulnerabilidades y los ataques a los sistemas de base de datos.

8. Práctica(s)

● Instalación y administración de un sistema de cortafuegos: ● Firewall por hardware ● Firewalls por software ● Crear un algoritmo de cifrado simétrico que permite colocar una contraseña a un mensaje. ● Se realizará Cifrado asimétrico donde a través de un manejador de claves del estándar GPG se creará la llave pública y privada para cifrar un documento. ● Instalar una VPN gratuita, con el propósito de extender una red a través de la internet de manera segura.

- Simular un dispositivo de seguridad con una lectora RFID y una laptop que permita conceder acceso o no a una persona.
- Instalación y administración de Base de datos con énfasis en la seguridad.
- Realizar ataques SQL injection a sistemas web con vulnerabilidades.
- Realizar respaldos y procesos de recuperación de sistemas de base de datos

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(s) de la asignatura, considerando las siguientes fases:

- **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.

- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.

- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de las competencias genéricas y específicas a desarrollar.

- **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesional, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación por competencias

Son las técnicas, instrumentos y herramientas sugeridas para constatar los desempeños académicos de las actividades de aprendizaje.

Para dicha evaluación de los alumnos, se cuenta con procedimientos y criterios que permitan dar seguimiento para evaluar los resultados del proceso de aprendizaje.

Los procedimientos y ponderación sugerida son:

- Tareas y participación activa en clases: 20%
- Exámenes para evaluar la comprensión de los temas: 20%
- Análisis de casos: 30%
- Prácticas: 30%

11. Fuentes de información

- Picouto Ramos, F. (2015) Seguridad perimetral monitorización y ataques en redes. Editorial Ra - Ma
- Ramos Varón, A. (2014) Hacking y seguridad de páginas Web. Editorial Ra - Ma
- Carballar Falcón, J. (2006) Firewall. La seguridad de la banda ancha. Editorial Ra - Ma.
- Lucena López, M. (2013) Criptografía y Seguridad en Computadores (4º ed), España: Editorial Universidad de Jaén.
- Libro Criptografia y Seguridad en Computadores:http://www.grc.upv.es/biblioteca/cripto.pdf
- Caballero Gil, P. (2002). Introducción a la criptografía (2ºed.). Madrid: Editorial RAMA
- Stinson, D.R. (2005). Cryptography: Theory & Practice (3ª ed.). Chapman and Hall
- Menezes, A. J. Van Oorschot P.C.& Vanstone, S.A. (2001). Handbook of Applied Cryptography. CRC Press.
- Pastor Franco, J. Sarasa López, M. y Salazar Riaño, J.L. (2001). Criptografía Digital: Fundamentos y aplicaciones. Zaragoza: Prensas Universitarias de Zaragoza.
- Gutiérrez, J. y Tena, J. (2003). Protocolos criptográficos y seguridad en redes. Servicio de publicaciones Universidad de Cantabria.
- Tilborg, V. (2000). Fundamentals of cryptology. Kluwer Academic Publishers.
- Resumen histórico sobre los hitos de la criptografía http://world.std.com/~cme/html/timeline.html
- Web de la agencia del departamento de comercio de EEUU del Instituto Nacional de Estándares y Tecnología http://www.nist.gov/itl/ y de la división de seguridad informática http://csrc.nist.gov/groups/STM/
- Servidor de Claves Públicas del MIT https://pgp.mit.edu/
- Artículo original del algoritmo RSA https://people.csail.mit.edu/rivest/Rsapaper.pdf
- Web para generar el par de claves (pública y privada) de cifrado https://gnupg.org/ Cómo enviar correos encriptados mediante Gmail http://www.enlanubetic.com.es/2012/11/enviar-correos-encriptados-en-gmail.html
- Información y algoritmo HASH http://www.secure-hash-algorithm-md5-sha-1.co.uk/
- El algoritmo de encriptación Blowfish https://www.schneier.com/cryptography/blowfish/
- Información sobre criptografía cuántica https://uwaterloo.ca/institute-for-quantumcomputing/research/areas-research/quantum-cryptography

- Centro Criptológico Nacional donde indica el nivel de alerta de ciberataques https://www.ccn-cert.cni.es/
- Instituto Nacional de Seguridad de España https://www.incibe.es/
- Revista de interés sobre criptografía a nivel internacional http://www.insaonline.org/
- La Fábrica Nacional de Moneda y Timbre emite el certificado electrónico que se puede utilizar para gestiones online http://www.cert.fnmt.es/
- Libro Criptografia y Seguridad: https://sindominio.net/metabolik/alephandria/txt/lucena_criptografia_y_seguridad.pdf.
- M. Peco.J. (2018) IoT con Raspberry Pi: Node-RED y MQTT, control de los GPIO con wiringPi y RPI, Python y C, UART, SPI, I2C, USB, Cámara, Sonido, etc.. CreateSpace Independent Publishing Platform
- Blokdyk Gerardus. (2017) Mobile Device Security Complete Self-Assessment Guide. Createspace Independent Publishing Platform.
- Murach, J. (2019). Murach's MySQL. (3a ed.). USA: Mike Murach & Associates, Inc.
- Malcher, M. (2019). Pro Oracle Database 18c Administration: Manage and Safeguard Your Organization's Data. (3a ed.). Huntley, IL., USA: Apress.
- Syverson, B. y Murach, J. (2020). Murach's SQL Server 2019 for Developers. USA: Mike Murach & Associates, Inc.
- Mike Murach & Associates, Inc.Syverson, B. y Nixon, R. (2020). Learning PHP, MySQL & JavaScript: With jQuery, CSS & HTML5. (5a ed.). USA: O'Reilly Media.