



1. Datos Generales de la asignatura

| | |
|---------------------------------|-------------------------------|
| Nombre de la asignatura: | Servicios seguros de internet |
| Clave de la asignatura: | CBD-2430 |
| SATCA¹: | 2-3-5 |
| Carrera: | Ingeniería en Ciberseguridad. |

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta el perfil del ingeniero en ciberseguridad las siguientes habilidades:

- Utiliza sistemas operativos, lenguajes de programación, redes y entornos tecnológicos para integrar soluciones de seguridad con responsabilidad e inclusión social en las organizaciones.
- Dirige el monitoreo, análisis y control de la información utilizando herramientas y marcos de referencia, con perspectiva ética, de respeto por la persona y de responsabilidad social.
- Diseña políticas de seguridad informática para establecer controles de seguridad pertinentes atendiendo los principios de no discriminación, Inclusión y equidad social.
- Gestiona incidentes y eventos de seguridad de informática para reducir la afectación negativa de la seguridad de la información y dar continuidad a las operaciones de la organización, atendiendo los principios de no discriminación, Inclusión y equidad social.
- Emplea métodos criptográficos para establecer protocolos de seguridad en el transporte de datos seguros a nivel de aplicación, usando herramientas de seguridad basadas en dichos protocolos integrando excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.
- Gestiona planes y proyectos de seguridad de la información de acuerdo con las necesidades del negocio, considerando riesgos y contingencias, promoviendo el cumplimiento de los principios de no discriminación, inclusión, equidad social, políticas, normas y acuerdos de nivel de servicio.
- Aplica procedimientos y técnicas de auditoría informática para detectar si se protegen los activos y recursos de la organización, si se mantiene la integridad de los datos, si se utiliza eficientemente los recursos, si se atienden los principios de no discriminación, inclusión y equidad social y si se cumple con las leyes y regulaciones establecidas.
- Implementa soluciones metodológicas y controles de seguridad en el ciclo de vida del desarrollo de software que permitan la reducción de vulnerabilidades y la inclusión de mejores prácticas de seguridad, con una perspectiva de responsabilidad social.

La asignatura “servicios seguros de internet” se centra en el estudio y aplicación de protocolos y buenas prácticas de los principales servicios que utilizamos en Internet. fomenta el desarrollo de habilidades para analizar, evaluar y mejorar los controles de seguridad de los servicios en línea, así como para diseñar soluciones efectivas, mitigar riesgos y amenazas contra ataques cibernéticos.

¹ Sistema de Asignación y Transferencia de Créditos Académicos



La asignatura es fundamental para la formación de profesionales de ingeniería en ciberseguridad, ya que los servicios de Internet se utilizan diariamente y se deben considerar la seguridad, como las vulnerabilidades de los servicios web, de correo electrónico, y la aplicación de medidas de protección adecuadas que incrementen la seguridad y la confidencialidad de la información en línea.

Intención didáctica

El contenido de esta materia se encuentra distribuido en cinco temas. Busca proporcionar al estudiante una comprensión profunda de los conceptos y técnicas necesarias para asegurar los servicios en línea de manera efectiva. Se pretende que el estudiante adquiera habilidades para implementar y gestionar servicios de Internet seguros, utilizando las mejores prácticas y estándares de seguridad adecuados.

En el tema uno, se familiarizará con los protocolos de internet y los desafíos de seguridad asociados con su uso. El estudiante comprenderá en profundidad los protocolos de comunicación en internet, como HTTP y HTTPS, y las vulnerabilidades comunes que pueden ser explotadas por atacantes. El estudiante podrá implementar medidas de seguridad para proteger la integridad, confidencialidad y disponibilidad de la información transmitida por estos protocolos y mitigar los efectos de ataques de denegación de servicio (DoS) mediante cortafuegos y filtros de paquetes.

En el tema dos, el estudiante obtendrá una comprensión detallada de los métodos de autenticación y autorización utilizados en los servicios en línea. Adquirirá conocimientos sólidos sobre diversos métodos de autenticación de usuarios, como contraseñas, tokens y biometría, además de los protocolos de autorización como OAuth y OpenID Connect. Desarrollará habilidades para implementar sistemas de autenticación seguros para gestionar adecuadamente los permisos de acceso de los usuarios en entornos en línea, incluyendo la gestión de identidades y accesos (IAM) en plataformas de servicios en la nube.

En el tema tres, el estudiante explorará los principios fundamentales de seguridad en aplicaciones web y las técnicas para protegerlas contra ataques cibernéticos. Entenderá las bases de la seguridad en aplicaciones web y la importancia de protocolos seguros.

En el tema cuatro, se proporcionan las herramientas para que el estudiante pueda proteger eficazmente los servicios de correo electrónico contra amenazas, garantizando la seguridad y confiabilidad de la comunicación electrónica en entornos empresariales y personales.

Finalmente, en el tema cinco, se busca que el estudiante pueda examinar los aspectos relacionados con la privacidad y la protección de datos en el entorno de Internet. Se espera que el estudiante adquiera conocimientos sobre técnicas de encriptación de datos en reposo y en tránsito, así como sobre prácticas para gestionar el consentimiento del usuario y cumplir con las regulaciones de privacidad.



3. Participantes en el diseño y seguimiento curricular del programa

| Lugar y fecha de elaboración o revisión | Participantes | Observaciones |
|--|--|--|
| Tecnológico Nacional de México del 4 al 6 de marzo del 2024. | Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas | Propuesta sintética de la carrera de Ingeniería en Ciberseguridad. |
| Tecnológico Nacional de México del 22 al 26 de abril del 2024. | Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas. Representante de Ciencias Básica de los Institutos de: Celaya, Morelia CENIDET y CIIDET. | Diseño y/o desarrollo curricular de la carrera de Ingeniería en Ciberseguridad |
| Tecnológico Nacional de México del 27 al 31 de mayo del 2024. | Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Jiquilpan, Mérida, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas | Consolidación curricular de la carrera de Ingeniería en Ciberseguridad. |

4. Competencia(s) a desarrollar

| Competencia(s) específica(s) de la asignatura |
|---|
| <ul style="list-style-type: none">Desarrollar una infraestructura de seguridad integral para proteger la privacidad y la integridad de los servicios en línea, aplicando protocolos de seguridad, técnicas de cifrado y autenticación, en los servicios utilizados en Internet. |



5. Competencias previas

- Conoce, selecciona y administra la seguridad de un sistema operativo en plataformas cliente-servidor, para resolver problemáticas reales y aplicar procedimientos de configuración de seguridad en plataformas de software.
- Describe, compara y analiza los diferentes métodos de enrutamiento aplicando normas y estándares internacionales para diseñar e implementar interconexiones de LAN's a través de WAN's.

6. Temario

| No. | Temas | Subtemas |
|-----|---|--|
| 1 | Seguridad en protocolos de Internet. | 1.1 Introducción a las vulnerabilidades en los protocolos de Internet. 1.2 Seguridad en el protocolo HTTP y HTTPS. 1.3 Protección contra ataques de denegación de servicio (DDoS). 1.4 Implementación de cortafuegos y filtros de paquetes. |
| 2 | Autenticación y autorización de servicios en línea. | 2.1 Sistemas de gestión de identidades y acceso. 2.2 Métodos de autenticación de usuarios (contraseñas, tokens, biometría). 2.3 Protocolos de autorización (OAuth, OpenID Connect, SAML). 2.4 Gestión de identidades y acceso (IAM) en entornos en la nube. |
| 3 | Seguridad en aplicaciones web. | 3.1 Principios de seguridad en aplicaciones web. 3.2 Amenazas y vulnerabilidades comunes en aplicaciones web. 3.3 Prevención de ataques comunes (SQL injection, XSS, CSRF). 3.4 Uso seguro de cookies y sesiones en aplicaciones web. 3.5 Validación de entradas y control de acceso a recursos. |
| 4 | Protección de servicios de correo electrónico. | 4.1. Seguridad en el protocolo SMTP y POP/IMAP. 4.2. Filtrado de spam y detección de phishing. 4.3. Implementación de cifrado de extremo a extremo. 4.4. Protección contra ataques de correo malicioso: ransomware y malware. 4.5. Análisis de bitácoras. 4.6. Aplicación de medidas de seguridad avanzadas (DKIM, SPF, DMARC). |



| | | |
|---|---|---|
| 5 | Privacidad y protección de datos en Internet. | <p>5.1 Normativas de privacidad y protección de datos.</p> <p>5.2 Cifrado de datos en reposo y en tránsito.</p> <p>5.3 Gestión de consentimiento del usuario y cumplimiento de regulaciones de privacidad.</p> <p>5.4 Protección de la privacidad en redes sociales y aplicaciones móviles.</p> |
|---|---|---|

7. Actividades de aprendizaje de los temas

| Tema 1. Seguridad en protocolos de Internet | |
|--|---|
| Competencias | Actividades de aprendizaje |
| <p>Específica(s): Aplicar los diferentes sistemas numéricos, como el binario, octal y hexadecimal.</p> <p>Genérica(s):</p> <ul style="list-style-type: none"> Habilidad de aplicar los conocimientos en la práctica. Habilidades en el uso de las tecnologías de la información y comunicaciones. Habilidad de investigación. Habilidad de aprender y actualizarse permanentemente. <p>Transversal(es):</p> <ul style="list-style-type: none"> Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano. | <ul style="list-style-type: none"> Investigar los incidentes de seguridad y/o vulnerabilidades que existen en los servicios de red que se encuentran en Internet. Abrir el dialogo sobre los hallazgos encontrados. Debatir sobre la importancia de proteger el transporte de algunos sitios web, creación de certificado SSL/TLS, informar sobre el procedimiento y las entidades de certificación autorizadas para ello. Explicar e implementar como se realiza un ataque de DoS y la forma de como mitigar los ataques de ese tipo; además, utilizar filtros de paquete con ayuda de un cortafuego. |



| Tema 2. Autenticación y autorización de servicios en línea | |
|--|---|
| Competencias | Actividades de aprendizaje |
| <p><i>Específica(s):</i> Implementar y gestionar sistemas de autenticación y autorización para garantizar la seguridad y la privacidad de los usuarios en entornos en la nube y servicios que requieran autenticación.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none">• Demuestra capacidad de abstracción, análisis y síntesis.• Demuestra capacidad de aplicar los conocimientos en la práctica.• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.• Demuestra capacidad para identificar, plantear y resolver problemas.• Demuestra capacidad para tomar decisiones.• Trabaja en equipo.• Habilidades interpersonales.• Habilidad para trabajar en forma autónoma.• Compromiso ético. <p><i>Transversal(es):</i></p> <ul style="list-style-type: none">• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano. | <ul style="list-style-type: none">• Investigar casos reales o simular algunos que involucren problemas de seguridad en servicios en línea. Se deberán analizar los casos, identificar los posibles puntos de vulnerabilidad y proponer soluciones de autenticación y autorización pertinentes.• Investigar y debatir sobre las herramientas que permite llevar a cabo el proceso AAA como Active directory, Openldap, OpenID Connect o soluciones IAM en la nube como AWS Identity and Access Management.• Realizar simulaciones de ataques de suplantación de identidad o intentos de acceso no autorizado a servicios en línea. Aplicar métodos seguros de autenticación e implementar con la autenticación multi-factor (tokens biométricos).• Análisis e investigación de protocolos de autenticación y autorización, como OAuth, OpenID Connect y SAML. |



| Tema 3. Seguridad en aplicaciones web | |
|---|--|
| Competencias | Actividades de aprendizaje |
| <p><i>Específica(s):</i> Analizar, identificar y aplicar principios de seguridad en aplicaciones web para prevenir y mitigar amenazas sobre vulnerabilidades comunes.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none">• Demuestra capacidad de abstracción, análisis y síntesis.• Demuestra capacidad de aplicar los conocimientos en la práctica.• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.• Demuestra capacidad para identificar, plantear y resolver problemas.• Demuestra capacidad para tomar decisiones.• Trabaja en equipo.• Habilidades interpersonales.• Habilidad para trabajar en forma autónoma.• Compromiso ético. <p><i>Transversal(es):</i></p> <ul style="list-style-type: none">• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano. | <ul style="list-style-type: none">• Investigar y discutir las principales vulnerabilidades que han sido explotadas en la Internet a los sitios web.• Montar un escenario de prueba como DVWA para probar las vulnerabilidades en sitios web: SQL Injection, XSS, CSRF, etc).• Realizar un programa de ejemplo en una plataforma web para que sanee las variables de entrada y evitar vulnerabilidades. |



| Tema 4. Protección de servicios de correo electrónico | |
|---|---|
| Competencias | Actividades de aprendizaje |
| <p><i>Específica(s):</i> Implementar y gestionar medidas de seguridad para proteger los servicios de correo electrónico contra amenazas cibernéticas.</p> <p><i>Genéricas:</i></p> <ul style="list-style-type: none">• Demuestra capacidad de abstracción, análisis y síntesis.• Demuestra capacidad de aplicar los conocimientos en la práctica.• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.• Demuestra capacidad para identificar, plantear y resolver problemas.• Demuestra capacidad para tomar decisiones.• Trabaja en equipo.• Habilidades interpersonales.• Habilidad para trabajar en forma autónoma.• Compromiso ético. <p><i>Transversal(es):</i></p> <ul style="list-style-type: none">• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano. | <ul style="list-style-type: none">• Montar un servidor de correo (SMTP) en una plataforma operativa como Unix, aplicando controles de seguridad sobre las vulnerabilidades a las que están expuestos los servicios de correo electrónico dentro de una red, como: malware, spam, falsificación, retransmisión falsa, servidores no autorizados dentro del mismo dominio, etc. |



| Tema 5. Privacidad y protección de datos en Internet | |
|---|--|
| Competencias | Actividades de aprendizaje |
| <p><i>Específica(s):</i> Implementar el cumplimiento de las regulaciones de privacidad y protección de datos en entornos digitales.</p> <p><i>Genéricas:</i></p> <ul style="list-style-type: none">• Demuestra capacidad de abstracción, análisis y síntesis.• Demuestra capacidad de aplicar los conocimientos en la práctica.• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.• Demuestra capacidad para identificar, plantear y resolver problemas.• Demuestra capacidad para tomar decisiones.• Trabaja en equipo.• Habilidades interpersonales.• Habilidad para trabajar en forma autónoma.• Compromiso ético. <p><i>Transversal(es):</i></p> <ul style="list-style-type: none">• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano. | <ul style="list-style-type: none">• Investigar y debatir la normativa de privacidad y protección de datos como: general data protection regulation, ley de protección de datos personales u otras leyes federales o locales aplicables.• Investigar y debatir las metodologías de cifrado de datos en reposo o en tránsito.• Mostar ejemplos de avisos de privacidad. Realizar un aviso de privacidad teniendo en cuenta los requisitos legales y las mejores prácticas de privacidad.• Investigar las políticas de privacidad de datos que tienen las redes sociales y las vulnerabilidades a que estamos expuestos. |



8. Práctica(s)

- Instalación de servidor web seguro con SSL/TLS.
- Implementación y configuración de medidas de seguridad en aplicaciones web y servicios en la nube.
- Instalación de servidor de correo electrónico con políticas de seguridad avanzada.
- Desarrollo de políticas de privacidad y cumplimiento normativo para servicios en línea.
- Implementación de políticas de seguridad para evitar la DoS.

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance del(los) logro(s) formativo(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 los saberes, habilidades y destrezas a desarrollar.

Evaluación: es la fase final que aplica un juicio de valor en el contexto laboral-profesión, 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”, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación de saberes, habilidades y destrezas

- Cuestionario.
- Rubrica de exposición.
- Guía de observación de ensayos.
- Guía de observación de reporte de práctica.
- Rubrica de investigación.



11. Fuentes de Información

1. Arroyo Miguel A. Seguridad en Internet: Cómo protegerse en el mundo digital.
2. Ballad Bill et al (2011). Access Control, Authentication, and Public Key Infrastructure. USA. Jones & Barttlet Learning LLC. Sullivan Bryan (2012). Web Application Security: A Beginner's Guide. New York. McGrawHill.
3. Bihis Charles (2015). Mastering OAuth 2.0. Packt Publishing Ltd.
4. Cross Michael (2014). Social Media Security: Leveraging Social Networking While Mitigating Risk. USA. Elsevier Inc.
5. De la Torre José A. Navegación segura por internet.
6. Fernández Juan Antonio y Del Río Luis Mariano. Seguridad en Internet y otros servicios web.
7. Kaplan James M. Ciberseguridad: Guía práctica para protegerse en el mundo digital.
8. Moreno Elio. Seguridad en redes sociales y dispositivos móviles.
9. Moreno Miguel Ángel. Ciberseguridad: Una guía para padres de familia y educadores.
10. Osmanoglu Ertem y Mena Jesus (2014). Identity and Access Management: Business Performance Through Connected Intelligence. USA. Elsevier Inc.
11. Porter Chris. Email Security with Cisco IronPort.
12. Sanz José Manuel. Seguridad en transacciones electrónicas: Guía de buenas prácticas.
13. Stallings William. Seguridad en Internet: Guía práctica para usuarios y profesionales.
14. Stuttard Dafydd y Pinto Marcus (2011). The Web Application Hacker's Handbook. Second edition. Canada. Wiley Publishing, Inc.
15. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI.