1. Datos Generales de la asignatura

Nombre de la asignatura:	Ciberseguridad
Clave de la asignatura:	CDH-2405
SATCA[1]:	1-3-4
Carrera:	Ingeniería en ciencia de datos

2. Presentación

Caracterización de la asignatura

Con el reciente auge de las tecnologías de información en cuanto a almacenamiento, acceso, procesamiento, privacidad, entre otras aplicaciones de la información, surge una necesidad imperante para asegurar, proteger y resguardar todo tipo de información que puede ser de carácter confidencial, como, por ejemplo: información gubernamental, información de proyectos de desarrollo, información médica, e información personal entre otros tipos.

Para el egresado en ingeniería en ciencia de datos, es de vital importancia que adquiera los conocimientos para generar o proponer las estrategias necesarias en materia de resguardo y protección de los datos, asegurando que el acceso a estos sea de acuerdo a los protocolos de seguridad que correspondan a la importancia y delicadeza de estos.

El alcance de los saberes para esta asignatura aporta al egresado en ingeniería en ciencia de datos capacidades y habilidades en el diseño de la arquitectura de datos en la nube y permitirá seleccionar los protocolos de seguridad adecuados para resguardar y asegurar la privacidad de los datos permitiendo así un acceso seguro para la visualización análisis y procesamiento de los mismos.

Intención didáctica

La asignatura de ciberseguridad se ubica en el quinto semestre de la ingeniería en ciencia de datos para contribuir al desarrollo de habilidades de análisis, síntesis de pensamiento crítico creativo y de compromiso ético. Dicha asignatura está conformada por cinco temas los cuales consisten en lo siguiente

Fundamentos de ciberseguridad, en este tema los alumnos obtendrán los conocimientos base que le permitirá diferenciar e identificar los diferentes conceptos que sirven de base para ciberseguridad, además de comprender la confidencialidad, integridad, disponibilidad y el análisis de riesgo.

En el tema de gobernanza, los alumnos adquirirán los conocimientos indispensables con respecto a la legislación con referencia a la ciberseguridad en nuestro país sus alcances los principales delitos informáticos en los que se incurre, así como de los diferentes sistemas de gestión de seguridad y las políticas y procedimientos estándares que actualmente rigen el comportamiento ético en la seguridad de datos.

En pruebas de penetración (pentesting) los alumnos obtendrán conocimientos de del hacking ético, así como diversas metodologías que le permitirán implementar las diversas fases del hackeo ético como la enumeración, detección de vulnerabilidades, explotación y escalamiento de privilegios; para

[1] Sistema de Asignación y Transferencia de Créditos Académicos

al final generar un reporte de los hallazgos encontrados y hacer pruebas de conceptos de ciberseguridad.

En el tema de endurecimiento de seguridad se procede a la instalación de controles y mecanismos que ayuden a mitigar los riesgos en ciber seguridad, por lo que se robustecen los servicios de red, puertos de comunicación (TCP/IP), seguridad perimetral (IPS/IDS), cero confianzas (endpoint), para finalizar en las actualizaciones (parches) y buenas prácticas para auditar la ciberseguridad de los sistemas que emplean ciencia de datos

Finalmente, en el tema de protección de datos, los alumnos conocerán e implementarán protocolos y herramientas de monitoreo, análisis de bitácoras, sistemas de respaldo y recuperación; así como métodos de cifrado y verificación (hash, criptografía pública y privada).

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico Superior de Alvarado del 21 al 23 agosto de 2023.	Representante del Instituto Tecnológico Superior de Alvarado.	Propuesta inicial.
Tecnológico Nacional de México 30 octubre 2023	Representante del Instituto Tecnológico de: Querétaro y del Instituto Tecnológico Superior de Alvarado.	Presentación de la propuesta de la carrera de Ingeniería en Ciencia de Datos.
Instituto Tecnológico de Querétaro Campus Norte del 19 al 22 de marzo 2024.	Representantes de los Institutos Tecnológicos de: Morelia, Puebla, Querétaro, Tehuacán. Instituto Tecnológico Superior de Alvarado. CENIDET. Representante de Ciencias Básica de los Institutos de: Celaya, Morelia y CIIDET.	Diseño y/o desarrollo curricular de la carrera de Ingeniería en Ciencia de Datos.
Tecnológico Nacional de México del 22 al 24 de abril del 2024	Representante del Instituto Tecnológico de Querétaro e Instituto Tecnológico Superior de Alvarado.	Contraste y ajuste de las asignaturas de Ingeniería en Ciencia de Datos con respecto a las de Ing. en Inteligencia Artificial, Ing. en Desarrollo WEB e Ing. en Ciberseguridad
Tecnológico Nacional de México del 27 al 31 de mayo del 2024.	Representantes de los Institutos Tecnológicos de: Morelia, Querétaro. Instituto Tecnológico Superior de Alvarado. CENIDET.	Consolidación curricular de la carrera de Ingeniería Ciencia de Datos

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Comprende los conceptos básicos de la ciberseguridad, para asegurar la integridad, la disponibilidad y la privacidad de los datos.

5. Competencias previas

- Conoce los principios y protocolos necesarios para el diseño y configuración de redes de computadoras.
- Comprende los fundamentos de los compromisos éticos en la materia de seguridad y el almacenamiento y cuidado de los datos.
- Programa aplicaciones empleando lenguajes de programación para ciencia de datos.

6. Temario

No.	Temas	Subtemas
1	Fundamentos de ciberseguridad.	1.1. Introducción a la ciberseguridad. 1.1.1. Vulnerabilidades. 1.1.2. Tipos de amenazas. 1.1.3. Ataques activos y pasivos. 1.1.4. Técnicas de mitigación. 1.1.5. Riesgos. 1.2. Ciberseguridad y seguridad de la información. 1.3. Objetivos de la seguridad informática (confidencialidad, integridad, disponibilidad). 1.4. Privacidad de la información. 1.5. AAA (autenticación, autorización y contabilidad). 1.6. Análisis de riesgo y mitigación.
2	Gobernanza.	2.1. Marcos de referencia de la ciberseguridad (ISO 27000, MAGERIT, MAAGTICSI, etc.). 2.2. Alcance y obligatoriedad. 2.3. Delitos informáticos. 2.4. Sistemas de gestión de seguridad. 2.5. Políticas, procedimientos, estándares y guías.
3	Pruebas de penetración (pentesting).	3.1. Definición de Etical hacking. 3.2. Metodologías. 3.3. Fases del hackeo ético integración de datos de múltiples fuentes. 3.3.1. Enumeración. 3.3.2. Detección de vulnerabilidades. 3.3.3. Explotación. 3.3.4. Escalación de privilegios. 3.4. Informe de vulnerabilidades 3.5. Pruebas de concepto

4	Endurecimiento de seguridad.	4.1. Servicios de red. 4.2. Puertos de comunicación (TCP/IP). 4.3. Actualizaciones (parches) y buenas prácticas. 4.4. Auditoría de seguridad. 4.5. Seguridad perimetral (IPS/IDS). 4.6. Cero confianzas (endpoint).
5	Protección de datos	5.1. Protocolos de monitoreo (SNMP). 5.2. Herramientas de monitoreo. 5.3. Análisis de bitácoras. 5.4. Sistemas de respaldo y recuperación. 5.5. Métodos de cifrado y verificación (hash, criptografía simétrica y asimétrica).

7. Actividades de aprendizaje de los temas

1. Fundamentos de ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): Conoce e identifica los fundamentos de ciberseguridad de los datos. *Genérica(s):* ● Capacidad de análisis y síntesis. ● Capacidad de organizar y planificar. ● Habilidad para buscar y analizar información proveniente de fuentes diversas. ● Toma de decisiones. ● Trabajo en equipo. ● Habilidades de investigación. ● Capacidad de generar nuevas ideas. ● Liderazgo. ● Habilidad para trabajar en forma autónoma. ● Búsqueda del logro.	● Reflexiona sobre la importancia de la seguridad de los datos en el medio. ● Realizar un mapa conceptual sobre ciberseguridad. ● Realiza una búsqueda de información sobre los tipos de riesgos y repercusiones en la ciberseguridad.
2. Gobernanza	
Competencias	Actividades de aprendizaje
Específica(s): Comprende el marco legal sobre ciberseguridad y sus alcances en los sistemas de gestión de seguridad. *Genéricas:* ● Capacidad de análisis y síntesis. ● Capacidad de organizar y planificar.	● Consulta información en diferentes fuentes con respecto al Marco legal de ciberseguridad en el país y en el extranjero. ● Realiza un cuadro de dos entradas sobre los diferentes delitos informáticos con sus características. ● Consultar información en diferentes fuentes sobre los sistemas de gestión de seguridad en el país. ● Realiza una infografía al respecto de las políticas, procedimientos y estándares en ciberseguridad.

• Habilidad para buscar y analizar información proveniente de fuentes diversas. • Toma de decisiones. • Trabajo en equipo. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma autónoma. • Búsqueda del logro.	• Se discute en una mesa y reflexiona sobre la importancia de regular el acceso a los datos por medio de la implementación de protocolos de ciberseguridad.
3. Pruebas de penetración (pentesting)	
Competencias	Actividades de aprendizaje
Específica(s): Utilizan los conceptos pruebas de penetración para realizar un informe de seguridad a través de la realización de las diversas fases del hackeo ético. *Genérica(s):* • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Toma de decisiones. • Trabajo en equipo. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma autónoma. • Búsqueda del logro.	• Escaneo de puertos usando herramientas como nmap (enumeración de puertos). • Desarrolla la enumeración de vulnerabilidades base de datos con inyección de código SQL con sqlmap. • Desarrolla un reporte con el análisis de vulnerabilidades usando burp, nmap, msfconsole • Realizar la explotación de vulnerabilidades usando herramientas nikto, msfconsole, nessus, entre otras. • Realizar el escalamiento de privilegios utilizando sistemas conocidos como vulnerables para prácticas de ciberseguridad (metasploitable, OWASP, etc.).
4. Endurecimiento de seguridad	
Competencias	Actividades de aprendizaje
Específica(s): Desarrolla un endurecimiento de servicios de red, protocolos de comunicación, equipos finales, seguridad perimetral, entre otros controles de ciberseguridad para la mitigación de riesgos. *Genérica(s):* • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas.	• Realización de un análisis de riesgos con herramientas automatizadas • Realización de la instalación de antivirus • Realizar la actualización y configuración de servicios de red como servidores web, base de datos, etc. • Realización de la aplicación de parches de seguridad y mejores prácticas de sistemas operativos y aplicaciones • Realizar la implementación de sistemas para la detección de intrusos (IDS), para la contención de ataques.

● Toma de decisiones. ● Trabajo en equipo. ● Habilidades de investigación. ● Capacidad de generar nuevas ideas. ● Liderazgo. ● Habilidad para trabajar en forma autónoma. ● Búsqueda del logro.	● Realizar la aplicación de firewall en los equipos y en la red. ● Implementar sistemas de autenticación como esquemas de 2 Fases, radius server, Kerberos, LDAP, etc. ● Propone esquemas de higiene cibernética.
5. Protección de datos	
Competencias	Actividades de aprendizaje
Específica(s): Aplica los mecanismos adecuados para la protección de datos. *Genéricas:* ● Capacidad de análisis y síntesis. ● Capacidad de organizar y planificar. ● Habilidad para buscar y analizar información proveniente de fuentes diversas. ● Toma de decisiones. ● Trabajo en equipo. ● Habilidades de investigación. ● Capacidad de generar nuevas ideas. ● Liderazgo. ● Habilidad para trabajar en forma autónoma. ● Búsqueda del logro.	● Realizar la implementación de políticas de respaldos y recuperación. ● Realizar la instalación y configuración de herramientas de monitoreo (Zabbix, nagios, etc.). ● Realizar el manejo de herramientas de cifrado simétrico y asimétrico. ● Usar herramientas de verificación e integridad de datos. Realizar la instalación y configuración de un sistema de criptografía de clave pública (PKI, SSL, VPN, etc.).

8. Práctica(s)

● Consultar un centro estatal de control, comando, comunicaciones y cómputo (C4), con el objetivo de conocer las buenas prácticas en el uso de tecnología de información. ● Realizar una conferencia o foro con integrantes de cuerpos de seguridad o policía cibernética, con el objetivo de informar sobre desarrollo de proyectos y buenas prácticas en el uso de tecnología de información. ● Configuración de protocolos de seguridad para la protección de datos. ● Aplica los mecanismos adecuados para la protección de datos empleando software o alguna aplicación que se desarrolló.

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

Para verificar el avance del desarrollo de saberes, habilidades y destrezas del alumno se sugiere solicitar:

Evidencias e instrumentos:

- Mapa conceptual-Rúbrica
- Mapa mental-Rúbrica
- Infografías–Lista de cotejo
- Reporte de búsqueda–Lista de cotejo
- Reportes de casos prácticas–Guías de observación
- Cuestionarios
- Rubricas de evaluación y listas de cotejo sobre las actividades desarrolladas por estudiantado.
- Exámenes escritos
- Discusiones sobre casos de estudio
- Rubricas de evaluación para presentaciones desarrolladas por el estudiantado
- Rúbricas de evaluación para organización de eventos en el aula por parte del estudiantado
- Participación/Exposiciones en clase
- Investigación documental
- Desarrollo y presentación de un proyecto. Rúbrica de Proyecto.
- Avances del Proyecto. Rúbrica de Proyecto.

11. Fuentes de información

1. Bird, J., Menzies, T., & Zimmermann, T. (2015). The art and science of analyzing software data: Analysis Patterns. Morgan Kaufmann.
2. Moustafa, A. A. (2022). Cybersecurity and cognitive science. Academic Press.
3. Rittinghouse, J. W., & Hancock, B. (2003). Cybersecurity Operations Handbook. Elsevier Digital Press
4. Rawat, D. B., & Ghafoor, K. Z. (2019). Smart Cities Cybersecurity and privacy. Elsevier
5. E.NAVARRO; V.PIATTINI. ”Auditoria Informática: Un enfoque practico”, RaMa.
6. Cert coordination Center, “Análisis de un sistema comprometido”. https://www.sei.cmu.edu/about/divisions/cert/index.cfm (accedido agosto 2022).
7. Sitio dedicado a la seguridad, Universidad Nacional Autónoma de México. http://www.seguridad.unam.mx (accedido agosto 2022).
8. Cert Coordination Center, Trabajo sobre el análisis de información en Unix, http://www.cert.org/tech_tips/win-UNIX-system_compromise.html (accedido agosto 2022).
9. Trabajo dedicado a la investigación forense en sistemas informáticos. http://www.loquefaltaba.com/documentacion/forense/ (accedido agosto 2022).
10. Trabajo sobre cómo hacer una auditoria informática, http://www.auditoria.com.mx/ (accedido agosto 2022).
11. Una colección de herramientas de un investigador forense. Utilidades escritas por
12. Chandan Kumar, https://geekflare.com/es/forensic-investigation-tools/ (accedido agosto 2022).
13. Scarfone K., Mell P., (2017) Guide to Intrusion Detection and Prevention Systems (IDPS),
14. NIST. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.
15. May C., Baker M., y Gabbard D., et. al., (2004), Advanced Information Assurance Handbook, CERT, Carnegie Mellon University, USA. http://www.cert.org/archive/pdf/aiahandbook.pdf.
16. Stoneburner G., Goguen A., Feringa A., (2001), Underlying Technical Models for Information Technology Security, NIST. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
17. Página principal de la metodología iso27000.es, http://www.iso27000.es (accedido agosto 2022).
18. EC-COUNCIL. “Digital Forensics Essentials”, EC-COUNCIL OFFICIAL CURRICULA, https://www.eccouncil.org/official/ (accedido agosto 2022).
19. Tevault Donald. Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Kindle Edition, 2018.
20. Miroshnikov Andrei. Windows Security Monitoring: Scenarios and Patterns. Ed. Wiley. 2018
21. Nemeth Evi, Snyder Garth. Unix and Linux system administration. Kindle Edition, 2017.
22. Sivarajan Santhosh. Getting Started with Windows Server Security. Kindle Edition, 2015.
23. Estándar internacional iso27000. http://www.iso27000.es (accedido agosto 2022).
24. "What is ESXI? | Bare Metal Hypervisor | ESX | VMware".
25. VMware. https://www.vmware.com/mx/products/esxi-and-esx.html (accedido el 30 de agosto de 2022).
26. "Open Source Cloud Computing Infrastructure - OpenStack".
27. OpenStack. https://www.openstack.org/ (accedido el 30 de agosto de 2022).
28. "Home - Docker". Docker. https://www.docker.com/ (accedido el 30 de agosto de 2022).
29. "Contenedores". Kubernetes. https://kubernetes.io/es/docs/concepts/containers/ (accedido el 30 de agosto de 2022).
30. "ISO 27001 - Software ISO 27001 de Sistemas de Gestión". Software ISO. https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/ (accedido el 30 de agosto de 2022).
31. "ISO 27001 - Seguridad de la información: norma ISO IEC 27001/2700

32. NIST, National Institute of Standards and Technology, NIST SP 800-123, Guide to General Server Security. 2022. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf
33. SANS, SysAdmin Audit, Networking and Security Institute. Políticas de seguridad para servidores. 2022. https://www.sans.org/information-security-policy/ (accedido agosto 2022).
34. Sitio dedicado a la seguridad, Universidad Nacional Autónoma de México. http://www.seguridad.unam.mx (accedido agosto 2022).
35. Seguridad de servicios web – Documentación de IBM 2022. https://www.ibm.com/docs/es/was-liberty/base?topic=applications-web-services-security (accedido agosto 2022).
36. Seguridad para los servicios básicos. 2022. https://docs.oracle.com/esww/iaas/Content/Security/Concepts/security_core_services.htm (accedido agosto 2022).
37. Seguridad de los servicios - WCF | Microsoft Docs. 2022. https://docs.microsoft.com/es-es/dotnet/framework/wcf/securing-services. (accedido agosto 2022).
38. Cisco Soluciones de Seguridad. 2022. https://www.cisco.com/site/mx/es/products/security/index.html (accedido agosto 2022).
39. Nemeth Evi, Snyder Garth. Unix and Linux system administration. Kindle Edition, 2017.
40. Tevault Donald. Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Kindle Edition, 2018.
41. Sivarajan Santhosh. Getting Started with Windows Server Security. Kindle Edition, 2015.
42. Miroshnikov Andrei. Windows Security Monitoring: Scenarios and Patterns. Ed. Wiley. 2018.
43. Krause Jordan. Windows Server 2016 Security, Certificates, and Remote Access
44. Cookbook: Recipe-based guide for security, networking and PKI in Windows Server 2016. Kindle Edition, 2018.
45. CIS, Center for Internet Security, Estándares y métodos de seguridad en SO. 2022. https://www.cisecurity.org/ (accedido agosto 2022).