1. Datos Generales de la asignatura

Nombre de la asignatura:	Fundamentos de Ciberseguridad
Clave de la asignatura:	CSF-2401
SATCA[1]:	*3-2-5*
Carrera:	Ingeniería en Sistemas Computacionales

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta al perfil del egresado la adquisición de los fundamentos de la Ciberseguridad, para satisfacer las necesidades de protección de la información de las organizaciones, con base en regulaciones y estándares internacionales, considerando aspectos de seguridad y calidad, con la finalidad de garantizar la integridad y disponibilidad de la información.

Es importante porque las habilidades que propicia en el estudiante permiten proteger las identidades personales y corporativas que utilizan el mundo tecnológico como medio de funcionamiento, obteniendo un sin número de oportunidades en empleos digitales en diversos sectores, para proteger la infraestructura tecnológica y la información que contiene.

Es por ello que el estudiante requiere de conocimientos en relación a criptología, gestión de riesgo y técnicas de hacking ético, que permitan anticipar la capacidad y vías de intrusión de un atacante.

Actualmente el Ingeniero en Sistemas Computacionales, debe tener la capacidad de diseñar e implementar sistemas seguros, para lo que son esenciales las técnicas de seguridad de equipos y aplicaciones, defensa perimetral, configuración de herramientas de protección y de los puestos finales de usuarios; seguimiento de alertas de ciberseguridad en el seno de los equipos especializados de respuesta a incidentes; así como el análisis de malware que puedan diseccionar un programa malicioso concreto.

Esta materia provee al alumno de conocimientos técnico-conceptuales básicos de ciberseguridad, que serán base para las materias contempladas en este módulo de especialidad.

Para el buen desarrollo de esta asignatura se requieren las competencias adquiridas en las materias de taller de sistemas operativos, de redes de computadoras, específicamente en el

[1] Sistema de Asignación y Transferencia de Créditos Académicos

funcionamiento y configuración de dispositivos de conectividad, su representación a través de los modelos OSI y TCP/IP, así como los protocolos de enrutamiento de paquetes de datos; también se requieren los conocimientos de análisis de riesgos, contenidos en la asignatura de gestión de proyectos de software.

Intención didáctica

El contenido de esta asignatura está integrado de cuatro temas:

En el primer tema, se definen conceptos básicos de ciberseguridad, se clasifican además los tipos de amenazas, riesgos y vulnerabilidades a que están expuestas las organizaciones y se describen mecanismos de defensa que pueden ser implementados. Las principales competencias genéricas a desarrollar en el estudiante a través de las diversas actividades que se realizarán en esta unidad son habilidades para buscar, procesar y analizar información procedente de fuentes diversas de gestión de información, así como la capacidad de organizar y planificar, con compromiso ético.

En el segundo tema, se estudian los principales controles de seguridad que pueden ser implementados a través de algoritmos de criptografía y criptoanálisis, así como de técnicas biométricas. Además, se destaca la importancia de las firmas y certificados digitales para asegurar la identidad de los firmantes y el no repudio. Estos contenidos contribuirán al desarrollo de competencias relacionadas con la gestión de información, capacidad crítica y autocrítica, compromiso ético, entre otras.

En el tercer tema, se analizan algunos contextos que como resultado de la transformación digital son objeto de riesgos que amenazan su seguridad, se identifican los principales ataques a que se exponen las redes, se analizan amenazas que puedan poner en peligro los servicios en la nube y los dispositivos conectados a internet.

Por último, en el cuarto tema, se destaca el uso de herramientas de Ciberseguridad aplicadas al comercio electrónico, utilizando análisis forense y hacking ético.

Las competencias genéricas más sobresalientes a desarrollar en el estudiante a través de las actividades que se realizarán en esta unidad son búsqueda, procesamiento y análisis de información procedente de fuentes diversas, capacidad crítica y autocrítica, así como toma de decisiones con compromiso ético.

El profesor deberá contar con experiencia en redes, seguridad informática e Industria 4.0 y haber participado en proyectos relacionados con estas áreas. Así mismo el profesor deberá identificar áreas de oportunidad en organizaciones de la región, mediante la vinculación del sector productivo y la institución, con el propósito de identificar proyectos basados en situaciones de Ciberseguridad, mediante los cuales sus estudiantes puedan conocer casos reales que les permitan adquirir una visión más amplia en este contexto.

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. Enero de 2024	M.G.T.I. Ayala Landeros Rosana D.C.C. González Lorence Armida M.C Morales Castro Claudia M.C.E. Rojo López Ariopajita M.G.T.I. Sánchez Saldaña Cristina M.G.T.I. Zozaya Salas Rocío Guadalupe	Reunión de Academia 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
Adquiere los fundamentos en Ciberseguridad, alineándolos a la organización, con base en los principios éticos, estándares y regulaciones nacionales e internacionales en la materia.

5. Competencias previas

- Diseña y configura redes informáticas aplicando estándares de comunicación.
- Aplica la gestión del análisis de riesgos
- Conoce, identifica, selecciona y administra diferentes sistemas operativos con el fin de resolver problemáticas reales, así como aplicar procedimientos de interoperabilidad entre diferentes sistemas operativos.
- Aplica los paradigmas de diseño de los sistemas operativos actuales y emergentes, para el manejo de los recursos del sistema.
- Diseña y elabora un proyecto de cableado estructurado aplicando normas y estándares vigentes para la solución de problemas de conectividad.
- Analiza los componentes y la funcionalidad de sistemas de comunicación para evaluar las tecnologías actuales como parte de la solución de un proyecto de conectividad.
- Diseña, instala y configura redes LAN inalámbricas aplicando normas y estándares vigentes para la solución de problemas de conectividad.

6. Temario

No.	Temas	Subtemas
1	Introducción a la Ciberseguridad	1.1 Conceptos, características y beneficios de la ciberseguridad. 1.2 Impacto de violación a la seguridad. 1.3 Tipos de amenazas, riesgos, ataques y vulnerabilidades. 1.4 Mecanismos de defensa. 1.5 El ciclo de la Ciberseguridad. 1.6 Estándares de ciberseguridad. 1.7 Casos famosos de Ciberseguridad.
2	Control de la Ciberseguridad	2.1 Diferencias entre seguridad informática y seguridad de la información. 2.2 Controles de seguridad. 2.3 Criptografía y criptoanálisis. 2.3.1 Tipos 2.3.2 Algoritmos 2.4 Firmas y certificados digitales. 2.5 Los cinco 9´s. 2.6 Técnicas biométricas.
3	Ciberseguridad en la Industria 4.0	3.1 Interconexión de redes. 3.2 IIOT 3.2.1 Nube. 3.2.2 Big Data. 3.2.3 IoT.
4	Herramientas de Ciberseguridad	4.1 Definición y herramientas 4.1.1 Análisis Forense. 4.1.2 Hacking ético. 4.1.3 E-Business

7. Actividades de aprendizaje de los temas

1. Fundamentos de la Ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): Identifica los riesgos y vulnerabilidades para el análisis de ciberataques, como medidas de prevención en la protección de datos y seguridad en las organizaciones. Genéricas:	● Caracterizar los ciberataques, ciberespacio, ciberseguridad, ciberamenaza, cibercrimen, privacidad, identidad, hacker, hackeo ético, hackctivismo, amenaza, ataque, riesgo, vulnerabilidad, seguridad, elaborando un cuadro comparativo.

• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. • Capacidad de organizar y planificar. • Capacidad de comunicación oral y escrita en su propia lengua. • Habilidad para trabajar de forma autónoma.	• Analizar las etapas del ciclo de un ataque, generando un reporte o un esquema. • Evaluar por equipos de trabajo el impacto de los diversos factores de riesgos y amenazas en una organización susceptibles a un ciberataque, elaborar en equipos una presentación ejecutiva y exponerla en plenaria para su análisis y discusión. • Realizar un cuadro sinóptico de los riesgos y amenazas más comunes actualmente (por ejemplo: robo de propiedad intelectual, defacements, extracción interna de datos, disponibilidad de los datos (DDos), inyecciones SQL, XSS, CSRF, LFI y RFI), enfatizar el impacto que pueden causar al interior de una organización. • Investigar sobre los diversos mecanismos de defensa, realizar un cuadro comparativo en la que se muestren cada uno de los mecanismos. • Investigar sobre el ciclo de la ciberseguridad y proponer un ciclo de vida de un ataque en un área específica (IoT, Cloud, SI, etc…). Elaborar en equipo una presentación ejecutiva y presentarla en plenaria para su análisis y discusión. • Analizar en sesión de mesa redonda los casos famosos de ciberseguridad, identificando los alcances del ciberataque y plantear los posibles mecanismos que debieron implementarse para evitar el ciberataque.
2. Control de la Ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): Analiza mecanismos de protección de datos en las organizaciones, que permitan la prevención de ciberataques.	• Presentar un informe de los antecedentes y conceptos de seguridad informática, así como sus elementos necesarios. • Realizar un cuadro comparativo de los diversos controles de seguridad que permitan eliminar riesgos informáticos.

Genéricas: ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Capacidad de organizar y planificar. ● Capacidad de comunicación oral y escrita en su propia lengua. ● Habilidad para trabajar en forma autónoma.	● Realizar el análisis del uso de algoritmos criptográficos en la generación de firmas electrónicas y certificados digitales, que ayuden a la autentificación de sitios seguros y elaborar una infografía. ● Investigar las técnicas biométricas que se utilizan actualmente en la protección de datos y elaborar una infografía. ● Caracterizar las cinco 9´s, de tal manera que les permitan saber su aplicación y elaborar un mapa mental.
3. Ciberseguridad en la Transformación Digital	
Competencias	Actividades de aprendizaje
Específica(s): Detecta factores de riesgo en los diversos elementos de la infraestructura tecnológica asociados a la digitalización para proveer seguridad informática a los activos de la organización Genéricas: ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Capacidad de organizar y planificar. ● Capacidad de comunicación oral y escrita en su propia lengua. ● Capacidad para tomar decisiones ● Capaacidad crítica y autocrítica.	● Caracterizar los principales ataques que pueden ser objetos las redes, mediante la elaboración de un cuadro sinóptico. ● Identificar los tipos de seguridad que pueden ser implementados en una red, lo expone en plenaria y socializa. ● Explicar la importancia de definir políticas de seguridad en la red mediante una presentación electrónica. ● Identificar amenazas y riesgos que pongan en peligro los servicios en la nube de las organizaciones, lo expone en plenaria y socializa. ● Seleccionar herramientas de big data utilizadas para anticipar posibles amenazas, elaborar un ensayo sobre su importancia. ● Investigar de qué manera se pueden aplicar disposiciones básicas de seguridad cibernética en los dispositivos conectados a internet de las organizaciones, mediante la elaboración de una presentación electrónica.
4. Herramientas de Ciberseguridad	
Competencias	Actividades de aprendizaje

Específica(s): Identifica herramientas de Ciberseguridad para fortalecer la protección y resiliencia de los recursos computacionales en las organizaciones. Genéricas: • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. • Capacidad de organizar y planificar. • Capacidad de comunicación oral y escrita en su propia lengua. • Capacidad para tomar decisiones • Capacidad crítica y autocrítica.	• Describir los pasos que se deben llevar a cabo una vez que se ha detectado una amenaza y se ha materializado, aplicando la técnica del análisis forense, utiliza para ello un diagrama de flujo. • Identificar aplicaciones críticas de las organizaciones que requieran ser protegidas para limitar el riesgo de seguridad, mediante la elaboración de un diagrama de llaves. • Destacar la importancia de los hackers éticos o expertos en pruebas de penetración de sistemas informáticos y de software con el fin de evaluar, fortalecer y mejorar la seguridad, elaborar un ensayo. • Utilizar herramientas para la protección de las diversas plataformas tecnológicas de posibles hackeos, elaborar reportes de prácticas.

8. Práctica(s)

- Configurar y administrar de manera correcta al menos 3 de los antivirus más comerciales. Incorporar en el reporte de práctica un cuadro comparativo en el que se destaquen sus fortalezas y vulnerabilidades.
- Desarrollar un programa que permita la encriptación y desencriptación de información.
- Instalar y configurar servicios en las redes de computadoras de manera física o virtual mediante herramientas de software (simuladores, máquinas virtuales, entre otros) y realizar la simulación de ataques al sistema de red.
- Configurar un Firewall físico o lógico.
- Realizar un análisis de red con alguna herramienta como por ejemplo un IPTraf, WireShark.
- Investigar y analizar incidentes de ciberseguridad.
- Crear y almacenar contraseñas seguras.
- Crear respaldos de datos en almacenamientos externos.
- Identificar comportamientos riesgosos en línea y proponer sugerencias de seguridad.
- Instalar herramientas de monitoreo de la red, que permitan identificar los tipos de paquetes que fluyen por la red, así como el origen y destino de estos (NetFlow Analyzer)
- Identificar las vulnerabilidades con el apoyo de herramientas e implementar las mejores prácticas para garantizar la continuidad de las operaciones, utilizando simuladores de red como Packet Tracer y GNS3

- Simular servicios en la nube con algunas plataformas que ya tienen adoptados los estándares de ciberseguridad (Google cloud, Amazon Web Services AWS, Microsoft Azure, entre otros)
- Seleccionar herramientas de software que permitan monitorear aplicaciones en la nube, dispositivos conectados a internet, plataformas de e-bussiness, etc.
- Conocer centros de datos en la región de alta disponibilidad y los estándares que aplican a sus operaciones.

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 comunitaria, 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 especificas 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”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación por competencias

Para la evaluación del aprendizaje 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: 30%
- Reportes de prácticas: 30%
- Portafolio de evidencias: 10%
- Exposiciones en clase:10%

Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar:

Listas de cotejo, listas de verificación, matrices de valoración, guías de observación, coevaluación y autoevaluación.

11. 11. Fuentes de información

Abad Parrales, W. M., Cañarte Rodríguez, T. C., Villamarin Cevallos, M. E., Mezones Santana, H. L., Delgado Pilozo, Á. R., Toala Arias, F. J., . . . Romero Castro, V.
F. (2019). *La ciberseguridad práctica aplicada a las redes, servidores y navegadores web* (Vol. Volumen 59 de Ingeniería y Tecnología). Alicante: 3Ciencias ISBN:8412116763, 9788412116762. doi:http://doi.org/10.17993/IngyTec.2019.59

Anglim, C. T. (2020). *Cybersecurity Legislation.* (I. Global, Ed.) New York: University of the District of Columbia, USA. doi:DOI: 10.4018/978-1-5225-9715-5.ch027

Arreola García, A. (2019). *Ciberseguridad: ¿Por qué es importante para todos?* México: Siglo XXI Editores México ISBN: 6070310411, 9786070310416.

BLANCO, U. (22 de noviembre de 2019). El Financiero. *Ciberseguridad en México: 9 ataques que amenazan en 2020*. Obtenido de https://www.elfinanciero.com.mx/tech

Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security, El Sevier, 88*(Juanuary 2020, 101607).

doi:https://doi.org/10.1016/j.cose.2019.101607

Cano, J. (2019). Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo. *SISTEMAS. Asociación Colombiana de Ingenieros de Sistemas.*, 63- 73. doi:10.29236/sistemas. n151a5

Carlo, A., Mantı, NP, WAM, BAS, Casamassima, F., Boschetti, N., Breda, P. y Rahloff, T. (2023). La importancia de los marcos de ciberseguridad para regular las tecnologías emergentes de IA para aplicaciones espaciales. Revista de ingeniería de seguridad espacial, 10 (4), 474-482.

Chang, K. y Huang, H. (2023). Explorando la gestión de redes multisectoriales de intercambio de información sobre ciberseguridad. Información Gubernamental Trimestral, 40 (4), 101870.

Chesney, B. (2020). *Chesney on Cybersecurity Law, Policy, and Institutions* (Vol. 3). Austin, Texas: University of Texas at Austin. Obtenido de https://ssm.com/abstract=3547103.

Chesney, R. (2020). *Cybersecurity Law, Policy, and Institutions (version 3.0).* Texas: University of Texas School of Law. doi:http://dx.doi.org/10.2139/ssrn.3547103.

Christen, M., Gordijn, B., & Loi, M. (2020). *The International Library of Ethics, Law and Technology, The Ethics of of Cybersecurity* (Vol. 21). Springer Nature, ISBN 978-3-030-29052-8 ISBN 978-3-030-29053-5. doi:https://doi.org/10.1007/978-3-030-29053-5

Dupont, B., Shearing, C., Bernier, M. y Leukfeldt, R. (2023). Las tensiones de la ciberresiliencia: del sentido a la práctica. Computadoras y seguridad, 132, 103372.

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V. y Knieps, M. (2023). Aprender de la ciencia de la seguridad: un camino a seguir para estudiar los incidentes de ciberseguridad en las organizaciones. *Computadoras y seguridad*, 103435.

ENCS (Estrategia Nacional de Ciberseguridad) de México. 2017. (31 de mayo de 2019). Obtenido de ENCS: https://bit.ly/2AEvAtU

Estañol, A. (23 de octubre de 2018). Expansión. *"La aseguradora AXA sufre un ciberataque en el Sistema de Pagos Electrónicos"*, págs. https://expansion.mx/empresas/2018/10/23/axa-sufre-un-ciberataque-en-el-spei.

Gupta, C., & Goyal, K. (2020). *Cybersecurity: A Self-Teaching Introduction.* Stylus Publishing, LLC ISBN: 1683924975, 9781683924975.

Haber, M., & Rolls , D. (2019). *The Three Pillars of Cybersecurity. In: Identity Attack Vectors.* Berkeley, CA: Apress, Berkeley, CA ISBN: 978-1-4842-5165-2, 978-

1- 4842-5164-5. doi:https://doi.org/10.1007/978-1-4842-5165-2_1

Jeimi , J., & Cano , M. (2020). Retos de seguridad/ciberseguridad en el 2030, Reflexión sobre un ejercicio prospectivo incompleto. *Sociedad 5.0 y tecnologías emergentes al 2030, 2020*(154). doi:https://doi.org/10.29236/sistemas. n154a7

Kävrestad, J., Rambusch, J. y Nohlberg, M. (2024). Principios de diseño para una formación en ciberseguridad cognitivamente accesible. Computadoras y seguridad, 137, 103630.

Kerttunen, M., & Eneken, T. (2020). *Routledge Handbook of International Cybersecurity.* Routledge ISBN: 1351038885, 9781351038881.

Lou, X., & Tellab, A. (2019). Cybersecurity Threats, Vulnerability and Analysis in Safety Critical Industrial Control System (ICS). *Recent Developments on Industrial Control Systems Resilience. Studies in Systems, Decision and Control, 255*, 75- 97. doi:https://doi.org/10.1007/978-3-030-31328-9_4.

McKinseyCompany. (junio de 2018). *Perspectiva de Ciberseguridad en México.* México: COMEXI.

Onwubiko, C., & Ouazzane, K. (2000). SOTER: A Playbook for Cybersecurity Incident Management. *IEEE Transactions on Engineering Management*, 1-21. doi:doi: 10.1109/TEM.2020.2979832.

Prümmer, J., van Steen, T. y van den Berg, B. (2023). Una revisión sistemática de los métodos actuales de formación en ciberseguridad. Computadoras y seguridad, 103585.

Shah, Y., Chelvachandran, N., Kendzierskyj, S., & Jahankhani, H. (april de 2020). 5G Cybersecurity Vulnerabilities with IoT and Smart Societies. (C. I. Springer, Ed.) *Advanced Sciences and Technologies for Security Applications*. doi:https://doi.org/10.1007/978-3-030-35746-7_9

Shoemaker, D., Kohnke, A., & Sigler, K. (2020). *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity.* New York: CRC Press ISBN: 1000050416, 9781000050417.

Sieber, S., & Zamora, J. (November de 2018). *The Cyber-security Challenge in a High Digital Density World. European Business Review.* Obtenido de https://www.europeanbusinessreview.com/the-cybersecurity-challenge-in-a-high- digital-density-world/

Sulich, A., Zema, T. y Kulhanek, L. (2023). Hacia un futuro seguro: un análisis bibliométrico de las relaciones entre ciberseguridad y desarrollo sostenible. *Procedia Informática*, *225*, 1448-1457.

Thakur, K., & Pathan, A.-S. K. (2020). *Cybersecurity Fundamentals: A Real-World Perspective.* Abindong,Oxon: CRC Press Taylor & Francis Group ISBN: 9780367476489.

Valdelamar, J. (16 de mayo de 2018). El Financiero. *"5 entidades y 300 mdp, involucrados en ciberataque: Banxico"*, págs. https://elfinanciero.com.mx/economia/5-entidades-fueron-afectadas-por-ciberataque-banxico.

Yeoh, W., Liu, M., Shore, M. y Jiang, F. (2023). Ciberseguridad de confianza cero: factores críticos de éxito y un marco de evaluación de madurez. Computadoras y seguridad, 133, 103412.

Zadeh, A., Lavine, B., Zolbanin, H. y Hopkins, D. (2023). Un marco de cuantificación y clasificación de riesgos de ciberseguridad para decisiones informadas de mitigación de riesgos. *Diario de análisis de decisiones*, *9*, 100328.