1. Datos Generales de la asignatura

Nombre de la asignatura:	**Estándares de Ciberseguridad**
Clave de la asignatura:	**CSF-2403**
SATCA[1]:	**3-2-5**
Carrera:	**Ingeniería en Sistemas Computacionales**

2. Presentación

Caracterización de la asignatura

La materia de Estándares de Ciberseguridad se ubica dentro del módulo de especialidad de la carrera de Ingeniería en Sistemas Computacionales como resultado del análisis del entorno en el que se encuentra inmerso el Tecnológico de San Juan del Río y como una respuesta a los eventos nacionales e internacionales que están ocurriendo con mucha frecuencia en lo relativo a “el hackeo” de información en muchos aspectos.

Debido a que la seguridad informática es una característica esencial en los actuales entornos computacionales, en donde el recurso de la información puede verse altamente comprometido si no se toman las medidas adecuadas de protección y preservación de datos, se hace necesario implementar diversos recursos que propicien una mayor seguridad en estos entornos.

Esta materia aporta al perfil del Ingeniero en Sistemas Computacionales los conocimientos y habilidades siguientes:

- Da soluciones a los problemas de diversos contextos.
- Coordina y participa en equipos multidisciplinarios para la aplicación de soluciones innovadoras.
- Evalúa tecnologías de hardware para soportar aplicaciones de manera efectiva y,
- Diseña, configura y administra redes de computadoras para crear soluciones de conectividad en la organización, aplicando las normas y estándares vigentes

Intención didáctica

La asignatura de Estándares de Ciberseguridad, introducirá al alumno a los marcos de referencia vigentes en cuestión de seguridad y protección de una organización; para ello se establecen los temas, la manera de abordarlos y su profundidad, con el fin de que al terminar el curso, el estudiante sea capaz de aplicar los conocimientos adquiridos que mitiguen o contrarresten los riesgos de seguridad.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

Como primer tema se encuentran los “Marcos de referencia”, que tienen como propósito que el estudiante interprete los estándares, legislaciones y regulaciones vigentes. El docente guiará al estudiante en el conocimiento de la terminología necesaria en los ámbitos de ciberseguridad. Se requiere que el estudiante tenga habilidades de búsqueda, procesamiento y análisis de grandes volúmenes de información, así como ser capaz de organizarse y planificar diversas actividades, trabajar de manera autónoma o en equipo y por ende una correcta comunicación tanto oral como escrita.

En la segunda unidad temática, “Plan de seguridad”, el estudiante debe ser capaz de elaborar un plan de seguridad aplicando una metodología de análisis y gestión de riesgos. Con la guía del docente, debe ser capaz de identificar los activos de la organización, sus vulnerabilidades, sus salvaguardas (mecanismos de seguridad) y estimar los riegos e impactos tanto potenciales como residuales (grado de riesgo y daño). Posterior al análisis, debe ser capaz de interpretar los valores de impacto y riesgo residual, determinará como se tratará el riesgo, si se va a eliminar, mitigar, compartir o aceptar, comunicando las decisiones, dándole seguimiento y haciendo revisiones a través de auditorías. Es importante señalar que el estudiante deberá demostrar su capacidad para la toma de decisiones y aplicación de conocimientos adquiridos.

Finalmente, la tercera unidad “Aplicación en Dominios de Ciberseguridad”, el docente ayudará al estudiante a identificar algunos dominios de ciberseguridad relacionados con la gestión de incidentes y plan de recuperación ante desastres para estar prevenidos y saber cómo actuar cuando nuestros activos son vulnerados para reestablecer la continuidad de las operaciones lo antes posible. Por último, se toca el tema de pentesting, esto es para que el alumno pueda analizar las vulnerabilidades de los activos y como se pueden corregir y esté consciente de la forma en que los hackers explotan dichas vulnerabilidades y cómo van ganando privilegios en los sistemas. En esta unidad temática, el alumno demostrará su capacidad en el manejo de diversas TIC y el aprendizaje autónomo.

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.	Ing. Medina Varela Wilfrido Lic. Rosales Álvarez Domingo M.G.T.I. Sánchez Saldaña Cristina Ing. Sánchez Orduña Govani Gregorio M.G.T.I. Vázquez Nieves Rogelio	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
Aplica marcos de referencia para la reducción de riesgos a través de un plan de seguridad.

5. Competencias previas

- Aplica fundamentos de ciberseguridad, alineándolos a la organización con base a los principios éticos, estándares y regulaciones nacionales e internacionales en la materia.
- Identifica estándares y normas legales nacionales e internacionales asociadas a la ciberseguridad.
- Identifica y selecciona estándares y métricas de calidad para ser aplicados a un proyecto de software.
- Aplica mecanismos de seguridad para proporcionar niveles de conformidad en una red.

6. Temario

No.	Temas	Subtemas
1	Marcos de referencia	1.1 Marco conceptual 1.1.1 Enfoque y organización 1.1.2 Amenazas y riesgos 1.1.3 Ataques 1.1.4 Vulnerabilidades 1.1.5 Ciberseguridad 1.1.6 SGSI 1.2 Marco teórico 1.2.1 Ciclo de Deming y mejora continua 1.2.2 Estándares 1.2.3 Mejores prácticas 1.3 Marco jurídico 1.3.1 Legislaciones 1.3.2 Regulaciones
2	Plan de seguridad	2.1 Método de análisis de riesgos 2.1.1 Caracterización de los activos 2.1.2 Caracterización de las amenazas 2.1.3 Caracterización de las salvaguardas 2.1.4 Estimación del estado de riesgo 2.2 Proceso de gestión de riesgos 2.2.1 Roles y funciones 2.2.2 Contexto 2.2.3 Criterios

		2.2.4 Evaluación de los riesgos 2.2.5 Decisión de tratamiento 2.2.6 Comunicación y consulta 2.2.7 Seguimiento y revisión 2.3 Proyectos de análisis de riesgo 2.4 Plan de seguridad
3	Aplicación en Dominios de Ciberseguridad	3.1 Gestión de incidentes 3.2 Recuperación ante desastres 3.3 Hacking ético 3.3.1 Recopilación de información 3.3.2 Identificación de vulnerabilidades 3.3.3 Explotación y hacking de vulnerabilidades 3.3.4 Técnicas de Post explotación

7. Actividades de aprendizaje de los temas

1. Marcos de referencia	
Competencias	Actividades de aprendizaje
Específica(s): Interpreta los estándares, legislaciones y regulaciones vigentes para intentar proteger y reducir riesgos cibernéticos a través del análisis de los marcos de referencia. Genéricas: ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Capacidad de organizar y planificar. ● Capacidad de comunicación oral y escrita ● Habilidad para trabajar en forma autónoma. ● Capacidad de trabajo en equipo ● Capacidad de análisis y síntesis.	● Elaborar un glosario de términos que incluya todos los conceptos vistos en el marco conceptual. ● Realizar un informe sobre las etapas del ciclo de Deming identificando actividades a realizar en cuestión de ciberseguridad. ● Investigar los estándares y normas actuales en cuestión de ciberseguridad. ● Realizar un cuadro sinóptico con cada uno de los estándares y normas, anteriormente investigados. ● Documentar buenas prácticas sobre ciberseguridad aplicadas a diversos ámbitos. ● Realizar una investigación sobre legislaciones y legislaciones existentes en ciberseguridad a nivel internacional, nacional y estatal.

<table>
<tr><td></td><td>

- Presentar en un foro el resultado de la investigación de legislaciones y regulaciones.

</td></tr>
<tr><td colspan="2">2. Plan de seguridad</td></tr>
<tr><td>Competencias</td><td>Actividades de aprendizaje</td></tr>
<tr><td>

Específica(s):

Aplica el proceso de gestión de riesgos, para su tratamiento a través de un plan de seguridad

Genéricas:

- Habilidad para buscar y analizar información proveniente de fuentes diversas.
- Capacidad para tomar decisiones.
- Capacidad de trabajo en equipo
- Capacidad de aplicar los conocimientos en la práctica
- Capacidad de comunicación oral y escrita

</td><td>

- Caracterizar los activos, sus vulnerabilidades, sus salvaguardas y estimar los riesgos e impacto tanto potencial como residual de un caso de estudio proporcionado por el profesor.
- Evaluar los riesgos e impacto residual y decidir cómo tratarlos, continuando con el caso de estudio
- Desarrollar un plan de seguridad del caso de estudio

</td></tr>
<tr><td colspan="2">3. Aplicaciones en Dominios de Ciberseguridad</td></tr>
<tr><td>Competencias</td><td>Actividades de aprendizaje</td></tr>
<tr><td>

Específica(s):

Establece estrategias usando mecanismos disponibles para dar solución a problemas en diversos dominios de ciberseguridad

Genéricas:

- Capacidad de aplicar los conocimientos en la practica
- Solución de problemas.
- Habilidad de uso de las tecnologías de la información y la comunicación
- Capacidad de aprender y actualizarse permanentemente.

</td><td>

- Desarrollar una guía para el manejo de incidentes de seguridad del caso de estudio
- Establecer políticas y/o procedimientos de recuperación de desastres del caso de estudio
- Analizar las posibles vulnerabilidades del caso de estudio a través de software de análisis de vulnerabilidades y utilizar técnicas para su explotación y post explotación. Proponer soluciones basadas en las recomendaciones indicadas por los organismos competentes en el tema

</td></tr>
</table>

8. Práctica(s)

- Realizar un mapeo de activos (físicos, de información, de servicios y personal) utilizando las herramientas disponibles de acuerdo al tipo de activo.
- Detectar vulnerabilidades mediante el uso de escáner de red, escáner de vulnerabilidades o software de pruebas de penetración automática.
- Implementar un IDS/IPS (SNORT, OSSEC, WinPatrol) y realiza un análisis de las intrusiones detectadas.
- Elaborar un protocolo de ciberseguridad-privacidad que contenga estrategias claves para proteger o mitigar las intrusiones a nivel acceso físico a dispositivos.

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 instrumentos de evaluación sugeridos son:

- Tareas y participación activa en clases.
- Exámenes para evaluar la comprensión de los temas.
- Reportes de prácticas.
- Portafolio de evidencias
- Exposiciones en clase

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. Fuentes de información

Asociación *Mexicana de Ciberseguridad.* (s.f.). Recuperado de https://www.ameci.org/

Declaratoria de vigencia de la Norma Mexicana NMX-I-27032-NYCE-2018. (s.f.). Recuperado de https://dof.gob.mx/nota_detalle_popup.php?codigo=5529046

Hernández, S. (2024). Curso completo de Hacking Ético y Ciberseguridad. Udemy. https://www.udemy.com/course/curso-completo-de-hacking-etico-y-ciberseguridad/?kw=curso+completo+de+hacking&src=sac

Harris Shon, Maymi Fernando. (2019). *CISSP – Exam Guide. Mc Graw Hill*

ISO / IEC 27032: 2023. (s.f.). *Tecnología de la información. Técnicas de seguridad. Directrices para la ciberseguridad. Recuperado* de Ciberseguridad https://www.iso.org/standard/76070.html

Incibe-cert , Boletín. (s.f.). Recuperado de https://www.incibe-cert.es/blog Inventario de activos y gestión de la seguridad en SCI. 29/12/2016, por INCIBE

LFPDPPP. (s.f.). Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ministerio de Hacienda y Administraciones públicas. (2012). Magerit – versión 3.0. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*.

Romero Castro Martha Irene, Figueroa Moran Grace Liliana. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades. Area de Innovación y Desarrollo.*

Sabillón, R. y Cano, J. J. (marzo, 2019). Auditorias de Ciberseguridad: Un modelo de aplicación general para empresas y naciones.

SecAware polices ( ) (S.f.). Recuperado de

https://www.iso27001security.com/html/toolkit.html .

Sector TIC, ISO 27001. (s.f.). Recuperado de Normas ISO: https://www.normas- iso.com/iso-27001/ (S.f.). Recuperado de https://www.sige.org.mx/producto/curso-de-la-norma-iso-27032-ciberseguridad/

Síntesis de protocolos de buenas prácticas y aplicación de competencias transversales y longitudinales en ciberseguridad-privacidad, Dr. Javier Areitio Bertolín. Director del Grupo de Investigación Redes y Sistemas. 27/05/2019 https://javierdisan.com/2018/09/25/guia- formacion-ciberseguridad/