1. Datos Generales de la asignatura

Nombre de la asignatura:	Estándares de Ciberseguridad
Clave de la asignatura:	SCF-2003
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, para

- Dar 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 alumno sea capaz de aplicar los conocimientos adquiridos que mitiguen o contrarresten los riesgos de infiltración.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

Como primer tema se encuentran los “Marcos de referencia”, que tienen como propósito que el alumno interprete los estándares, legislaciones y regulaciones vigentes. El docente guiará al alumno en el conocimiento de la terminología necesaria en los ámbitos de ciberseguridad. Se requiere que el alumno 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, “Riesgos”, el alumno debe ser capaz de aplicar el proceso de gestión de riesgos, a fin de dar un tratamiento a través del modelo de auditoría de dicho proceso. Para lograr esto, el alumno debe ser consciente de la necesidad de contar con seguridad en cada ente/elemento/servicio de uso habitual con el cual se tenga interacción directa dentro de una organización; Con la guía del docente, debe ser capaz de caracterizar los riesgos cibernéticos más populares o comunes que se presentan en las organizaciones, identificar el grado de daños o en su caso los elementos que sean comprometidos durante la gestión de los riesgos; el docente también debe guiar al alumno en el conocimiento o identificación de los posibles mecanismos de protección que pueden ser aplicados para minimizar los riesgos o sus efectos, haciendo uso de herramientas o estándares de gestión de proyectos como SCRUM o KANBAN; también será capaza de desarrollar un plan para la implementación del proceso de gestión de riesgos en una organización o área específica, que pueda ser evaluado o monitoreado a través de un proceso de auditoría de ciberseguridad. Es importante señalar que el alumno 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 alumno a identificar algunos dominios de ciberseguridad relacionados con la gestión de riesgos que le permitan proponer estrategias a través del uso de diversos mecanismos disponibles dentro de una organización o del entorno del dominio y así mismo lo guiará en la propuesta de las soluciones, con base en las legislaciones, estándares y normas vigentes; estableciendo un control/manejo adecuado de riesgos que permita la continuidad de las operaciones. 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. Junio del 2020.	Ing. Gómez Muñoz Roberto M.G.T.I. Sánchez Saldaña Cristina Ing. Sánchez Orduña Govani Gregorio Lic. Rosales Álvarez Domingo M.E. Trejo García Leticia M.G.T.I. Vázquez Nieves Rogelio	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
Aplica marcos de referencia para la solución de problemas de seguridad y protección de la privacidad a través de la gestión de incidentes.

5. Competencias previas

Adquirir los 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	Riesgos	2.1 Riesgos de seguridad y protección

		privacidad 2.2 Proceso de gestión de riesgos 2.2.1 Establecimiento del contexto de gestión de riesgos de seguridad de la información 2.2.2 Valoración de riesgos de seguridad de la información 2.2.3 Tratamiento de riesgos de seguridad de la información 2.2.4 Monitoreo, revisión y comunicación de riesgos de seguridad de la información 2.3 Auditoría en Ciberseguridad (CSAM)
3	Aplicación en Dominios de Ciberseguridad	3.1 Identificación de vulnerabilidades 3.2 Riesgos cibernéticos 3.3 Gestión de incidentes 3.4 Recuperación ante desastres

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 identificar las vulnerabilidades 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. • Comunicación oral y escrita en su propia lengua. • Habilidad para trabajar en forma autónoma. • Trabajo en equipo • Capacidad de abstracción, análisis y síntesis.	• Elabora un glosario de términos que incluya todos los conceptos vistos en el marco conceptual. • Realiza un informe sobre las etapas del ciclo de Deming identificando actividades a realizar en cuestión de ciberseguridad. • Investiga los estándares y normas actuales en cuestión de ciberseguridad. • Realiza un cuadro sinóptico con cada uno de los estándares y normas, anteriormente investigados. • Documenta buenas prácticas sobre ciberseguridad aplicadas a diversos ámbitos. • Realiza una investigación sobre legislaciones y legislaciones existentes en ciberseguridad a nivel internacional, nacional y estatal. • Presenta en un foro el resultado de la investigación de legislaciones y regulaciones.

<table>
<tr><th colspan="2">2. Riesgos</th></tr>
<tr><th>Competencias</th><th>Actividades de aprendizaje</th></tr>
<tr><td>Específica(s):

Aplica el proceso de gestión de riesgos, para su tratamiento a través del modelo de auditoría de ciberseguridad

Genéricas:

• Habilidad para buscar y analizar información proveniente de fuentes diversas.
• Toma de decisiones.
• Trabajo en equipo
• Capacidad de aplicar los conocimientos en la práctica
• Comunicación oral y escrita en su propia lengua.</td><td>• Caracteriza los riesgos cibernéticos más populares o comunes que se presentan en las organizaciones, donde se visualice el grado de daños o elementos comprometidos y cuáles son los mecanismos de protección contra ellos.
• Aplica un instrumento a diferentes usuarios, para identificar el grado de consciencia sobre la seguridad digital y privacidad de su información, al realizar diversos trámites o hacer uso de servicios cotidianos.
• Desarrolla un plan para la implementación del proceso de gestión de riesgos.
• Elabora un plan de auditoria de ciberseguridad.</td></tr>
<tr><th colspan="2">3. Aplicaciones en Dominios de Ciberseguridad</th></tr>
<tr><th>Competencias</th><th>Actividades de aprendizaje</th></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.
• Manejo de tecnologías de información y comunicación
• Capacidad de aprender y actualizarse permanentemente.</td><td>• Analiza las posibles vulnerabilidades y propone soluciones basadas en estándares para establecer el tratamiento de dichas vulnerabilidades en la infraestructura tecnológica de una pequeña a mediana empresa.
• Diseña estrategias para el manejo de riesgos y amenazas de ciberseguridad para la organización, elaborando una descripción detallada de la propuesta de cómo abordarlos y que controles propone.
• Establece políticas y/o procedimientos de recuperación de desastres en la organización.</td></tr>
</table>

8. Práctica(s)

- Realiza un mapeo de activos (físicos, de información, de servicios y personal) utilizando las herramientas disponibles de acuerdo al tipo de activo.
- Detecta vulnerabilidades mediante el uso de escáner de red, escáner de vulnerabilidades o software de pruebas de penetración automática.
- Implementa un IDS/IPS (SNORT, OSSEC, WinPatrol) y realiza un análisis de las intrusiones detectadas.
- Desarrolla una aplicación que gestione el control de acceso privado a aplicaciones web desde equipos móviles utilizando autenticación multifactor.
- Elabora 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 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 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

Andrés Alvares, A. y Fernández Sánchez, C. M. (s.f.). Guía Práctica de ISO/IEC 20000-1 para servicios TIC. AENOR Ediciones

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

Cisco*(estandar) (s.f) recuperado de https://www.cisco.com/c/dam/global/es_es/products/security/pdfs/estandares_minimos_de_seguridad.pdf*

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

Gómez Fernández, L. y Fernández Rivero, P. P. (s.f.). Cómo implantar un SGSI según UNE ISO/IEC 27001:2014 y sus aplicaciones en el esquema nacional de seguridad. AENOR Ediciones.

ISO 27001. (s.f.). Recuperado de ISOTools EXCELLENCE: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISO / IEC 27032: 2012. (s.f.). *Tecnología de la información. Técnicas de seguridad. Directrices para la ciberseguridad. Recuperado* de https://www.iso.org/standard/44375.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.

Ley de la Propiedad Industrial. (s.f.). Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/50_180518.pdf

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

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/

Sige ( ) (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/