Seguridad de Sistemas Computacionales
Carta al Estudiante

Características del curso

Sigla: CI-0143.
Nombre del Curso: Seguridad de Sistemas Computacionales.
Semestre: I-2022.
Programa: Bachillerato en Computación.
Créditos: 4.
Horas lectivas: 5.
Requisitos: CI-0122 Sistemas Operativos, CI-0121 Redes de Comunicación de Datos, CI-0123 Proyecto Integrador de Sistemas Operativos y Redes de Comunicación de Datos, CI-0127 Bases de Datos, CI-0126 Ingeniería de Software, y CI-0128 Proyecto Integrador de Ingeniería de Software y Bases de Datos.
Correquisitos: ninguno.
Clasificación: curso propio.
Ciclo de carrera: I ciclo, 4to año (énfasis de Ingeniería de Tecnologías de la Información) y II ciclo, 4to año (énfasis de Ingeniería de Software y electiva del énfasis de Ciencias de la Computación).
Horario de clase: K 16:00-17:50/ V 15:00-17:50 en la plataforma BBB de la NAC.
Horario consulta: K 15:00-19:00, M 17:00-18:00, J 17:00-18:00,
la consulta es en la Oficina Virtual de la NAC,
previa cita el día anterior, otros horarios a convenir
Grupo: 01.
Profesor: Ricardo Villalón Fonseca (ricardo.villalon@ucr.ac.cr)
Oficina: Oficina Virtual en la plataforma BBB de la NAC, será publicada por el docente a los estudiantes, al inicio del curso.

Descripción del curso

Este es un curso básico de seguridad de la información con un enfoque que mezcla lo teórico y lo práctico. Se tratarán ideas y conceptos básicos de seguridad, análisis de riesgos, controles y métodos de protección y pruebas. El curso genera conciencia en el estudiante sobre la necesidad de aplicar de forma continua la seguridad a los sistemas computacionales.

Objetivo General

El *objetivo general* del curso es que cada estudiante entienda o aplique conceptos de seguridad de la información y de seguridad de infraestructura tecnológica, para atender los requerimientos de seguridad de los sistemas computacionales, utilizando análisis, controles y métodos de protección, mediante ejemplos prácticos, proyectos o asignaciones.

Objetivos Específicos

Durante este curso, cada estudiante:

1. Comprenderá las ideas y conceptos básicos de seguridad para fundamentar las decisiones que se toman en materia de seguridad.
2. Realizará, a partir de los objetivos de seguridad de una organización, el análisis de riesgos para definir y priorizar los requerimientos técnicos de seguridad.
3. Aplicará resultados de un análisis de riesgos de seguridad para determinar el tratamiento y la priorización de los riesgos.
4. Conocerá e implementará controles y métodos de protección para mitigar riesgos identificados en el análisis según las prioridades definidas.
5. Ejecutará pruebas de seguridad para determinar que la mitigación de riesgos fue efectiva.

Objetivos transversales

6. Comunicará efectivamente sus resultados, tanto de manera escrita como oral.
7. Practicará habilidades de trabajo en equipo.

Contenido temático

Los ejes temáticos del curso y los objetivos a los que contribuyen se muestran a continuación:

1. Fundamentos de seguridad de sistemas digitales (objetivo 1)

- Definición de seguridad.
- Confidencialidad, integridad, disponibilidad, autenticación, autorización, responsabilización (“accountability”), no repudio, auditoría
- Objetivos de seguridad.
- Riesgos: vulnerabilidad, amenaza, probabilidad de materialización, impacto, relación costo-beneficio.
- Cadena de ataque (“*kill-chain*”)
- Modelos de seguridad (por ejemplo McCumber).

2. Análisis de requerimientos (objetivo 2)

- Requerimientos de: negocio, tecnología, actores e involucrados, normativa, información y aplicaciones.

3. Análisis de riesgos de seguridad (objetivo 3)

- Identificación de vulnerabilidades, amenazas, activos, controles, consecuencias.
- Evaluación de riesgos, metodología cualitativa y cuantitativa.
- Tratamiento: modificación, evasión, retención y reparto.

4. Controles y métodos de protección (objetivo 4)

- Políticas y procedimientos
- Criptografía: simétrica, asimétrica, irreversible, fundamentos de criptografía de llave pública (PKI)
- Mecanismos de identidad y acceso (IAM)
- Seguridad en redes: seguridad perimetral, canales seguros (por ejemplo: VPN, TLS/SSL), monitorización de redes
- Seguridad de aplicaciones: ataques a aplicaciones de software, programación defensiva (por ejemplo, validación de entradas, aserciones, técnicas de manejo de errores), con base en una clasificación y priorización de la industria.
- Seguridad en computadores y servidores: reforzamiento ("hardening"), aislamiento y confinamiento (virtualización y cajas de arena)

5. Pruebas de seguridad (objetivo 5)

- Análisis de vulnerabilidades y pruebas de penetración.
- Análisis y evaluación de seguridad (estático y dinámico)

Metodología

La modalidad del curso es alto virtual. El curso se realizará mediante clases virtuales sincrónicas, con espacios para discusión, comentarios de los estudiantes y solución de problemas. También se desarrollarán algunas actividades asincrónicas. El estudiante aplicará los conceptos por medio de tareas cortas, tareas programadas/laboratorios, proyectos, u otros tipos de evaluaciones.

Durante el semestre se abrirán espacios para presentar proyectos cortos de investigación realizados por los estudiantes, con respecto a temas relacionados a los objetivos del curso. Los temas de investigación serán asignados y presentados en grupos, la dinámica de las presentaciones será definida al inicio del curso.

Material de lectura para estudio se lista en la bibliografía, pero la misma será complementada con lecturas y ejemplos adicionales de otras fuentes.

Evaluación

Evaluación	Porcentaje
Tareas programadas/ proyectos aplicados	65%
Tareas y evaluaciones cortas o investigaciones	20%
Trabajo final	15%
Total	100%

Para aprobar el curso el estudiante debe obtener al menos 67.5 puntos al finalizar el semestre. Si la nota final está entre 57.5 y 67.4 tendrá derecho a realizar un examen de ampliación. En este examen el estudiante deberá obtener una nota mínima de 70.0 para aprobar el curso. En caso de que obtenga una nota menor a 57.5, o de presentar el examen de ampliación con una nota inferior a 70.0 reprobará el curso.

Las tareas cortas, investigaciones, tareas programadas, laboratorios y proyectos deberán ser entregados el día definido en cada tarea a más tardar a media noche. Entregas tardías serán penalizadas con un 5% de la nota obtenida en la evaluación durante el primer día de atraso, un 10% adicional por el segundo día, y un 15% adicional por el tercer día, para un máximo de 30% de penalización por entrega tardía. La evaluación se considerará como no entregada luego de este tiempo. Extensiones en los tiempos de entrega sin penalización pueden ser concedidos solamente por el profesor del curso y para casos excepcionales.

Logística

Todo el material a evaluar, las fechas y contenidos de las evaluaciones, así como los anuncios importantes relacionados a actividades del curso serán dados durante las lecciones virtuales o presenciales, por lo tanto se recomienda fuertemente la asistencia de forma regular. En caso de tener que ausentarse a alguna lección, es responsabilidad del estudiante ponerse al día en lo que corresponda a material y aspectos administrativos del curso. Puede hacer uso de las horas de consulta del profesor para obtener información de los puntos más relevantes de una lección a la que no haya podido asistir, pero queda en la responsabilidad del estudiante estudiar el material completo y detalles del caso.

Se utilizará la plataforma educativa de la UCR http://mediacionvirtual.ucr.ac.cr, la Nube Académica Computacional y otros recursos tecnológicos disponibles en la UCR como apoyo para proveer material digital para el curso, como recordatorio de las evaluaciones, y para anunciar y coordinar las actividades del curso. El estudiante debe matricularse en los sistemas que se provean para poder acceder al material digital.

Cronograma

Cant. Semanas	Tema	Evaluación
2	1	Presentación
2	2	Tarea/Proy.
2	3	Tarea/Proy.
5	4	Tarea/Proy.
2	5	Tarea/Proy.
2		Trab. final

Bibliografía

- Anderson, R. **"Security Engineering: A Guide to Building Dependable Distributed Systems"**. 3ra edición, Wiley, 2020
- Bejtlich, R. **"El TAO de la monitorización de seguridad en redes"**. Pearson Educación, S.A., 2005.
- Clarke, J. "**SQL Injection Attacks and Defenses"**. Syngress Publishing, 2009.
- Du, W. **"Computer & Internet Security. A Hands-on Approach"**. 2a edición, 2019.
- Fernández, E. B. **"Security Patterns in Practice"**. Wiley, 2013.
- Harris, S, y Maymi, F. **"CISSP all-in-one exam guide"**. McGraw-Hill Education, 8va edición, 2019.
- Hoglund G. y McGraw G. **"Exploiting Software: How to break code"**. Addison-Wesley, 2004.
- Howard, M. y LeBlanc D. **"Writing Secure Code"**, 2da edición. Microsoft Press Redmond, 2002.
- McClure, S., Scambray, J. **"Hacking Exposed: Network Security Secrets & Solutions"**. Osborne, 7ma edición, 2012.
- McConnell S. **"Code Complete"**. 2da edición. Microsoft Press Redmond, 2002.
- McCumber, J. **"Assessing and Managing Security Risk in IT Systems: A structured methodology"**. Auerbach, 2005.
- Pfleeger, C.P. **"Security in computing"**. 4a edición. Prentice Hall, 2007.
- Schneier, B. **"Applied cryptography: protocols, algorithms, and source code in C"**. 2da edición. Wiley, 1996.
- Shackleford, D. **"Virtualization Security: Protecting Virtualized Environments"**. Sybex, 2013.

Recursos estudiantiles

Para información sobre recursos estudiantiles disponibles en la UCR, incluyendo el Sistema de bibliotecas y la normativa universitaria vigente, favor visitar la página https://www.ecci.ucr.ac.cr/vida-estudiantil/servicios-institucionales-para-estudiantes/guia-de-recursos-estudiantiles-de-la-ucr