

Programa del curso EE-8808

Fundamentos de ciberseguridad

Escuela de Ingeniería Electromecánica
Carrera de Ingeniería Electromecánica con énfasis en Sistemas Ciberfísicos

I parte: Aspectos relativos al plan de estudios

1. Datos generales

Nombre del curso:	Fundamentos de ciberseguridad
Código:	EE-8808
Tipo de curso:	Teórico
Obligatorio o electivo:	Obligatorio
Nº de créditos:	1
Nº horas de clase por semana:	2
Nº horas extraclase por semana:	1
Ubicación en el plan de estudios:	Curso de 8 ^{vo} semestre en Ingeniería Electromecánica con énfasis en Sistemas Ciberfísicos
Requisitos:	Ninguno
Correquisitos:	EE-8807 Aplicaciones de sistemas embebidos
El curso es requisito de:	<i>Énfasis en Sistemas Ciberfísicos:</i> EE-9302 Desarrollo de software para aplicaciones críticas
Asistencia:	Libre
Suficiencia:	Sí
Posibilidad de reconocimiento:	Sí
Aprobación y actualización del programa:	01/01/2026 en sesión de Consejo de Escuela 01-2026

2. Descripción general

El curso de *Fundamentos de ciberseguridad* aporta en el desarrollo del siguiente rasgo del plan de estudios: desarrollar aplicaciones de sistemas embebidos integrados en sistemas electromecánicos.

Los aprendizajes que los estudiantes desarrollarán en el curso son: aplicar medidas de ciberseguridad en el diseño de sistemas ciberfísicos, garantizando la protección de datos y la integridad de las aplicaciones.; implementar protocolos de seguridad en sistemas ciberfísicos, asegurando la confiabilidad y resiliencia de los dispositivos y redes; y desarrollar soluciones de protección mediante programación y criptografía, aplicando técnicas de cifrado, automatización de tareas de seguridad y herramientas para la detección y mitigación de riesgos.

Para desempeñarse adecuadamente en este curso, los estudiantes deben poner en práctica lo aprendido en los cursos de: Microcontroladores, y Fundamentos de organización de computadoras.

Una vez aprobado este curso, los estudiantes podrán emplear algunos de los aprendizajes adquiridos en el curso de: Aplicaciones de Inteligencia Artificial.

3. Objetivos

Al final del curso la persona estudiante será capaz de:

Objetivo general

- Comprender los principios fundamentales de la ciberseguridad aplicados al diseño y desarrollo de sistemas ciberfísicos..

Objetivos específicos

- Aplicar medidas de ciberseguridad en el diseño de sistemas ciberfísicos, garantizando la protección de datos y la integridad de las aplicaciones..
- Implementar protocolos de seguridad en sistemas ciberfísicos, asegurando la confiabilidad y resiliencia de los dispositivos y redes.
- Desarrollar soluciones de protección mediante programación y criptografía, aplicando técnicas de cifrado, automatización de tareas de seguridad y herramientas para la detección y mitigación de riesgos.

4. Contenidos

En el curso se desarrollaran los siguientes temas:

1. Introducción a la ciberseguridad
 - 1.1. Historia y evolución de la ciberseguridad
 - 1.2. Principios básicos de ciberseguridad
 - 1.3. Importancia de la ciberseguridad en el mundo actual
2. Redes y protocolos
 - 2.1. Tipos de redes (LAN, WAN, MAN)
 - 2.2. Protocolos de comunicación (TCP/IP, HTTP, HTTPS, MQTT)
 - 2.3. Seguridad en redes: firewalls y sistemas de detección de intrusos (IDS/IPS)
3. Programación para la ciberseguridad

- 3.1. Scripts y automatización para la seguridad informática
- 3.2. Ejercicios prácticos de programación para detectar y mitigar vulnerabilidades
- 4. Amenazas y vulnerabilidades
 - 4.1. Tipos de amenazas (malware, phishing, ataques DDoS)
 - 4.2. Análisis de vulnerabilidades y gestión de parches
 - 4.3. Uso de software antivirus y antimalware
- 5. Criptografía
 - 5.1. Fundamentos de criptografía (simétrica y asimétrica)
 - 5.2. Aplicaciones prácticas del cifrado en la protección de datos
 - 5.3. Implementación de técnicas de cifrado en proyectos prácticos
- 6. Seguridad en redes
 - 6.1. Configuración y gestión de firewalls
 - 6.2. Seguridad en redes inalámbricas (WPA2, WPA3)
 - 6.3. Control de acceso y autenticación multifactor (MFA)
- 7. Seguridad en aplicaciones
 - 7.1. Desarrollo seguro de software (principios y prácticas)
 - 7.2. Pruebas de penetración y análisis de seguridad en aplicaciones web
 - 7.3. Herramientas y técnicas para asegurar aplicaciones
- 8. Gestión de incidentes
 - 8.1. Respuesta a incidentes de ciberseguridad
 - 8.2. Recuperación y análisis forense
 - 8.3. Estudios de caso de incidentes reales y lecciones aprendidas
- 9. Cumplimiento y normativas
 - 9.1. Normativas y estándares de ciberseguridad (ISO 27001, GDPR)
 - 9.2. Políticas de seguridad y su implementación
 - 9.3. Evaluación de cumplimiento y auditorías de seguridad

II parte: Aspectos operativos

5. Metodología En este curso, se utilizará el enfoque sistémico-complejo para la ejecución de las sesiones magistrales y se integrará la investigación práctica aplicada para las asignaciones extraclase. Esta última se implementará mediante técnicas como el estudio de casos, el aprendizaje basado en proyectos, el modelado y la simulación.

Las personas estudiantes podrán desarrollar actividades en las que:

- Recibirán clases magistrales con material audiovisual y discusión en grupo sobre conceptos fundamentales de ciberseguridad.
- Desarrollarán proyectos integradores que fomenten la colaboración y el aprendizaje interdisciplinario, permitiéndoles trabajar en equipos para abordar problemas complejos e integrar conocimientos de diferentes áreas de la ciberseguridad.
- Resolverán ejercicios de diagnóstico y autoevaluación relacionados con vulnerabilidades, criptografía y cumplimiento normativo, para monitorear su progreso en la identificación de amenazas, el uso de técnicas de cifrado y la aplicación de estándares de seguridad.
- Realizarán pruebas de penetración controladas sobre aplicaciones y servicios simulados, con el fin de identificar vulnerabilidades, aplicar técnicas de análisis y proponer soluciones basadas en buenas prácticas de desarrollo seguro.
- Llevarán a cabo actividades de investigación orientadas a fomentar el pensamiento crítico y la capacidad de análisis, investigando nuevas amenazas y técnicas de ciberseguridad para mantenerse actualizados con las últimas tendencias del sector.

Este enfoque metodológico permitirá a la persona estudiante comprender los principios fundamentales de la ciberseguridad aplicados al diseño y desarrollo de sistemas ciberfísicos.

Si un estudiante requiere apoyos educativos, podrá solicitarlos a través del Departamento de Orientación y Psicología.

6. Evaluación La evaluación se distribuye en los siguientes rubros:

- Pruebas parciales: evaluaciones formales que miden el nivel de comprensión y aplicación de los conceptos clave del curso. Generalmente cubren una parte significativa del contenido visto hasta la fecha y pueden incluir problemas teóricos y prácticos.
- Pruebas cortas: evaluaciones breves y frecuentes que sirven para comprobar el dominio de temas específicos. Suelen ser de menor peso en la calificación final y permiten reforzar el aprendizaje continuo.
- Act. aprendizaje activo: actividad diseñada para que los estudiantes se involucren de manera directa y práctica en la construcción de su conocimiento, a través de la resolución de problemas, la discusión y la aplicación de conceptos teóricos en contextos reales o simulados.

Pruebas parciales (2)	60 %
Pruebas cortas (5)	25 %
Act. aprendizaje activo (4)	15 %
Total	100 %

De conformidad con el artículo 78 del Reglamento del Régimen Enseñanza-Aprendizaje del Instituto Tecnológico de Costa Rica y sus Reformas, en este curso la persona estudiante tiene derecho a presentar un examen de reposición si su nota luego de redondeo es 60 o 65.

7. Bibliografía

- [1] W. Stallings y L. Brown, *Computer Security: Principles and Practice*, 4.^a ed. Pearson, 2018.
- [2] D. Stuttard y M. Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, 2.^a ed. Wiley, 2011.
- [3] W. Stallings, *Network Security Essentials: Applications and Standards*, 5.^a ed. Pearson, 2013.
- [4] J. Erickson, *Hacking: The Art of Exploitation*, 2.^a ed. No Starch Press, 2008.

8. Persona docente

El curso será impartido por:

Herson Esquivel Vargas, Ph.D.

Bachillerato en Ingeniería en Computación, Instituto Tecnológico de Costa Rica, Costa Rica

Maestría en Ciencias de la Computación con énfasis en Telemática, Instituto Tecnológico de Costa Rica, Costa Rica

Maestría en Ciencias de la Computación con énfasis en Ciberseguridad, Instituto Kerckhoffs - Universidades de Twente, Eindhoven y Nijmegen, Holanda

Correo: h.esquivelvargas@itcr.ac.cr Teléfono: 88131925

Oficina: 13 Escuela: Ingeniería en Computación Sede: Cartago