GUÍA DOCENTE

Curso Avanzado
Privacidad y
Seguridad en IoT

EEN002

Alejandra Miguel
López

NOMBRE DEL CURSO	Curso Avanzado Privacidad y Seguridad en IoT
CÓDIGO	EEN002
MODALIDAD	Formación eLearning
TIPOLOGÍA DE LA TITULACIÓN	Cursos avanzados 80-150 horas
ÁREA DE CONOCIMIENTO	Ciberseguridad
PROFESORADO	Alejandra Miguel López
CORREO DE CONTACTO CON EL PROFESORADO	formacion.amiguel@ciberin.es
TUTORÍAS	Concretar cita con los profesores
IDIOMA EN EL QUE SE IMPARTE	Español
ADAPTADO A PERSONAS CON DISCAPACIDAD	Sí, a petición

ÍNDICE

1. Resumen del Curso y Objetivos

1.1. Resumen del Curso

El curso avanzado de Privacidad y Seguridad en IoT está diseñado para proporcionar a los estudiantes los conocimientos fundamentales para mejorar la seguridad y privacidad en dispositivos IoT, con un enfoque en buenas prácticas, herramientas forenses y cumplimiento normativo. A lo largo de este curso, los estudiantes adquirirán las competencias necesarias para desarrollar habilidades prácticas de cara a proteger tanto datos personales como dispositivos conectados.

1.2. Objetivos del Curso

- Comprensión de los conceptos básicos de IoT y su impacto en la seguridad y privacidad.
- Profundización en la implementación de buenas prácticas y estrategias de protección de la privacidad y gestión de datos en entornos IoT.
- Desarrollo de habilidades para la identificación de las principales amenazas y vulnerabilidades en dispositivos IoT.
- Conocimiento de tendencias emergentes y desafíos futuros en la seguridad de IoT.

2. Competencias

2.1. Competencias Generales

- Evaluación de los riesgos y vulnerabilidades en dispositivos IoT.
- Identificar amenazas emergentes y desarrollar estrategias de mitigación efectivas basadas en el análisis de riesgos y amenazas.
- Implementación de buenas prácticas y dominio de recomendaciones de seguridad para la protección de la privacidad y gestión de datos en entornos IoT.

2.2. Competencias Específicas

- Configurar y gestionar dispositivos IoT de forma segura.
- Aplicar medidas de protección de la privacidad y los datos.
- Implementar protocolos de seguridad en redes IoT.
- Cumplir con normativas y regulaciones internacionales de seguridad y privacidad.
- Conocimiento especializado de ataques informáticos a dispositivos IoT y respuestas ante ellos.

3. Contenidos

3.1. Contenidos Teóricos

- **Tema 1. Introducción**: concepto y evolución, características, funcionamiento y arquitectura, categorías de dispositivos IoT, tecnologías de comunicación IoT.

- **Tema 2. Vulnerabilidades de los dispositivos IoT**: conceptos, permisos, fuga de privacidad, falta de seguridad en fabricación, dirección MAC estática, falta de autenticación y control de la seguridad física, desventajas de las conexiones Bluetooth, falta de normas, modo broadcast, caso Strava.

- **Tema 3. Ataques a dispositivos IoT**: áreas de ataque, ataques más frecuentes, casos de ataques.

- **Tema 4. Medidas, mecanismos, recomendaciones de seguridad e investigación forense de IoT**: propiedades de seguridad, protocolos, legislaciones y estándares, metas de mitigación de riesgos de alto nivel, requisitos críticos para la seguridad en entornos IoT, vulnerabilidades más críticas de los dispositivos IoT y recomendaciones, investigación forense de IoT.

- **Tema 5. Futuro de la seguridad IoT**: tendencias emergentes, desafíos y oportunidades.

3.2. Contenidos Prácticos

3.2.1. Ejercicios Teórico-Prácticos

- Ejercicio 1 (Tema 2): Análisis de vulnerabilidades.
- Ejercicio 2 (Tema 3): Identificación de ataques.
- Ejercicio 3 (Tema 4)
    - Reflexión límites privacidad dispositivos IoT.
    - Implementación marco de seguridad.
- Ejercicio 4 (Tema 5)
    - Análisis ventajas y desventajas tecnologías emergentes.
    - Investigación tecnología emergente.

3.3. Trabajo final

Análisis de un caso práctico utilizando los conocimientos adquiridos a lo largo del curso. Se proporcionará al alumno un caso a analizar y realizará su estudio para su resolución mediante la identificación de los ataques, las vulnerabilidades, las medidas y recomendaciones de seguridad, las técnicas de investigación forense para analizar el ataque y la implementación de un Marco de Ciberseguridad.

Resumen contenido teórico	Total de horas
TEORÍA	15h
EJERCICIOS TEÓRICO-PRÁCTICOS	12h
TRABAJO FINAL	15h

4. Estrategias Metodológicas, Materiales y Recursos Didácticos

4.1. Estrategias Metodológicas

- Clases teóricas:
  - Clases virtuales con presentación PPT en las que se explicará cada tema y se expondrán ejemplos y casos.
  - PDFs con la teoría vista en las clases, de forma desarrollada.
- Discusiones y aportaciones en el foro: planteamiento de temas y cuestiones a resolver y debatir en el foro.
- Ejercicios teórico-prácticos individuales: ejercicios con cuestiones para poner en práctica lo estudiado en cada tema utilizando distintas herramientas para resolver casos forenses.
- Tests: parciales de cada tema y uno general del curso.

4.2. Materiales y Recursos Didácticos:

- Lecturas recomendadas: material complementario para ampliar lo visto en las clases y guías para aprender a utilizar otras herramientas forenses.
- Artículos científicos: estudios para la preparación del trabajo final y complementar los temas presentados.
- Videos educativos: ejemplos de las explicaciones para facilitar la realización de las prácticas, charlas y otros vídeos de interés acerca de los temas estudiados.
- Software especializado: aportación de las herramientas estudiadas en cada tema para cada práctica.

5. Evaluación

5.1. Criterios de Evaluación

- **Comprensión Teórica:** Se evaluará la capacidad del estudiante para entender y explicar los conceptos teóricos presentados en el curso. Esto incluye la precisión en las respuestas y la claridad en la exposición de ideas.
- **Aplicación Práctica:** Se valorará la habilidad del estudiante para aplicar los conocimientos teóricos a situaciones prácticas y resolver problemas específicos relacionados con el contenido del curso.
- **Participación Activa:** Se tendrá en cuenta la participación del estudiante en las actividades del curso, incluyendo su contribución en los foros de discusión, la formulación de preguntas pertinentes y la interacción con sus compañeros y el profesor.
- **Calidad del Trabajo Final:** Se evaluará la profundidad del análisis, la originalidad, la estructura y la presentación del trabajo final del curso. Esto incluye la correcta aplicación de la metodología y el rigor científico.
- **Resolución de Ejercicios Prácticos:** Se valorará la precisión y la eficacia en la resolución de los ejercicios prácticos propuestos, así como la capacidad para seguir las instrucciones y aplicar los procedimientos adecuados.
- **Desempeño en Pruebas y Exámenes:** Se evaluará el rendimiento del estudiante en las pruebas y exámenes realizados durante el curso, teniendo en cuenta la exactitud de las respuestas y la demostración de un conocimiento sólido de los temas tratados.
- **Autonomía y Responsabilidad:** Se considerará la capacidad del estudiante para gestionar su propio aprendizaje, cumplir con los plazos de entrega y demostrar responsabilidad en la realización de las tareas asignadas.

5.2. Criterios de Calificación

- **1.- Exámenes de cada tema:** 10%
  2.- Examen Final de Curso: 15%
- **3- Ejercicios de diferentes unidades/temas:** 30%
- **4.- Participación activa en el foro (cuestiones moderadas por el tutor, participación en resolución de dudas, feedback varios, etc):** 10%
- **5.- Ejercicio práctico tutorizado (Actividad práctica):** 15%
- **6.- Trabajo final:** 20%

(Necesario superar 50% de puntos 1, 2, 3, 5 y 6, y 100% punto 4).

6. Cronograma

Semana 1 – Tema 1 (11h y 45 min)

- PPT presentación (15 min)
- PPT tema (30 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (3 horas)
- Vídeos (1 hora)

Semana 2 – Tema 2 (14h y 45 min)

- PPT tema (30 min)
- PPT explicación práctica (15 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (3 horas)
- Ejercicio práctico (3 horas)
- Vídeos (1 hora)

Semana 3 – Tema 3 (14h y 45 min)

- PPT tema (30 min)
- PPT explicación práctica (15 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (3 horas)
- Ejercicio práctico (3 horas)
- Vídeos (1 hora)

Semana 4 – Tema 4 (14h y 45 min)

- PPT tema (30 min)
- PPT explicación práctica (15 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (3 horas)
- Ejercicio práctico (3 horas)
- Vídeos (1 hora)

Semana 5 – Tema 5 (14h y 45 min)

- PPT tema (30 min)
- PPT explicación práctica (15 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (3 horas)
- Ejercicio práctico (3 horas)
- Vídeos (1 hora)

Semana 6 (17h y 45 min)

- PPT explicación trabajo final (15 min)
- PPT repaso test final (30 min)
- Trabajo final (15 horas)
- Test final (2 horas)

Semana	Clases Grabadas (teoría + explicación prácticas)	PDFs teoría	Lecturas recomendadas	Foro	Ejercicios Prácticos	Trabajo final del curso	Documentales /videos	Test	**Total**
1	45 min	3h	3h	3h			1h	1h	**11h y 45 min**
2	45 min	3h	3h	3h	3h		1h	1h	**14h y 45 min**
3	45 min	3h	3h	3h	3h		1h	1h	**14h y 45 min**
4	45 min	3h	3h	3h	3h		1h	1h	**14h y 45 min**
5	45 min	3h	3h	3h	3h		1h	1h	**14h y 45 min**
6	45 min					15h		2h	**17h y 45 min**
Total	**4h y 30 min**	**15h**	**15h**	**15h**	**12h**	**15h**	**5h**	**7h**	**90h**

7. Bibliografía

7.1. Lecturas Obligatorias

- Glosario de términos de Ciberseguridad. INCIBE
- Marco de Ciberseguridad. NIST

7.2. Lecturas Recomendadas

- Internet of Things (IoT) of Smart Homes: Privacy and Security. Magara T., Zhou Y. Journal of Electrical and Computer Engineering. Hindawi. 2024.
- Análisis de vulnerabilidades en los sistemas de información de los equipos LG SMART TV que utilizan aplicaciones IoT. Cristian D., William L., Claudia Y., Héctor M. Fundación Universitaria Los Libertadores.
- Ciberseguridad en los dispositivos iot de uso doméstico: una revisión sistemática de la literatura. Alexander X., Javier D. Revista Científica Arbitrada Multidisciplinaria. Vol. 7, Núm. 1, 2025, Pág. 140-170.

- Domótica y Privacidad: Navegando entre la Comodidad Tecnológica y la Seguridad de los Datos. Inés, Y., Universidad Internacional de La Rioja. 2024.
- Las 20 contraseñas más usadas en España y en el mundo (tablas). 2023. Bankinter. URL: https://www.bankinter.com/blog/finanzas-personales/contrasenas-mas-usadas-espana-mundo
- A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. Sasi T., Habibi A., Lu R., Xiong P., Iqbal S. Journal of Information and Intelligence. 2024. Págs. 455-513.
- DDoS attack detection techniques in IoT networks: a survey. Pakmehr, A., Abmuth A., Taheri N., Ghaffari A. Cluster Computing. 2024.
- Using machine learning algorithms to enhance IoT system security. Hosam E., Samir A., Omar H., Belgacem B. Scientific reports. 2024.
- Seguridad en Dispositivos IoT para Redes LoRa. Martínez D. Universidad de los Andes. 2023.
- Ganar en competitividad cumpliendo el RGPD: guía de recomendaciones para empresas. INCIBE.
- The Internet of Things in the Era of Generative AI: Vision and Challenges. Wang X., Wan Z., Hekmati A., Zong M., Alam S., Zhang M., Krishnamachari B. Generative AI for the Internet of Things. IEEE Internet Computing Magazine. 2024.
- A review of IoT applications in healthcare. Li C., Wang J., Wang S., Zhang Y. Neurocomputing. Elsevier. 2024

8. Información Adicional

8.1. Requisitos Previos

- Este curso está dirigido a aquellos estudiantes o graduados en informática, criminalística, criminología o cualquier otra titulación relacionada con el ámbito informático forense.
- En caso de no disponer de una titulación relacionada con este ámbito, será necesario que el estudiante posea conocimientos básicos de informática

8.2. Políticas del Curso

Al inscribirse en este curso, los participantes reconocen haber leído, entendido y aceptado las políticas siguientes:

- El participante acepta que utilizará las herramientas y conocimientos adquiridos en el curso únicamente para fines legales y éticos, por lo que exonera a la institución, al profesor y a cualquier entidad asociada de cualquier responsabilidad derivada del uso inapropiado de dichos conocimientos.
- Si el estudiante necesita adaptaciones especiales o tiene dificultades de aprendizaje, deberá informar al profesorado al inicio del curso para proporcionar el apoyo necesario y adecuar el contenido y los materiales.
- Los documentos propios del curso deben de manejarse con uso restringido, es decir, que no se permite compartir material propio de Ciberin Security S.L. con terceros o difundirlo públicamente (manuales de estudio, videos, clases grabadas, etc.).

Ciberin Security S.L. no se hace responsable por el uso inadecuado o ilegal de las herramientas y técnicas enseñadas en este curso, siendo los participantes los únicos responsables de sus acciones y de las consecuencias legales que puedan derivarse del uso inadecuado de la información y habilidades adquiridas.

Por lo que, cualquier actividad que implique la violación de la privacidad de terceros, la infiltración en sistemas o cuentas sin autorización y cualquier otro acto que contravenga la ley, será considerado una violación grave de los términos de este curso y resultará en la expulsión inmediata y en la notificación a las autoridades competentes."