Guía docente de la asignatura

Diseño de Sistemas Software Seguros (M52/56/4/4)

Fecha de aprobación por la Comisión Académica: **19/07/2024**

Máster	Máster Universitario en Desarrollo del Software
MÓDULO	• Diseño y Desarrollo de Servicios y Sistemas • Diseño y Desarollo de Servicios y Sistemas
RAMA	Ingeniería y Arquitectura
CENTRO RESPONSABLE DEL TÍTULO	Escuela Internacional de Posgrado

Semestre	Primero	**Créditos**	3	**Tipo**	Obligatorio	**Tipo de enseñanza**	Enseñanza Virtual

PRERREQUISITOS Y/O RECOMENDACIONES

Ninguno.

BREVE DESCRIPCIÓN DE CONTENIDOS (Según memoria de verificación del Máster)

- Fundamentos de seguridad y privacidad en sistemas software.
- Análisis de amenazas e implementación de contramedidas.
- Etapas en la protección de los sistemas software: Prevención, detección, respuesta y análisis.
- Principios y buenas prácticas de diseño de software seguro.
- Metodologías y técnicas para el desarrollo de software seguro.
- Aplicación de tecnologías actuales (por ejemplo, Blockchain) en seguridad.

- Fundamentals of security and privacy in software systems.
- Analysis of threats and implementation of countermeasures.
- Stages in the protection of software systems: Prevention, detection, response and analysis.
- Principles and good practices of secure software design.
- Methodologies and techniques for the development of secure software.
- Application of current technologies (for example, Blockchain) in security.

COMPETENCIAS

COMPETENCIAS BÁSICAS

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
- CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

RESULTADOS DE APRENDIZAJE (Objetivos)

Conocimientos o contenidos

C08. Conoce las características principales de los sistemas del internet de las cosas, su arquitectura, los elementos que lo componen y su rol en el sistema, su capacidad de conectividad, y los requerimientos necesarios para su implementación en cuanto a la confiabilidad, rendimiento, seguridad o escalabilidad.

C011. Comprende los principios y fundamentos de diseño de software seguro, identificando las vulnerabilidades y amenazas que pueden afectar a cualquier tipo de sistema software.

Competencias

COM4. Evaluar los diferentes aspectos e implicaciones (sociales, legales, seguridad, éticos, ecológicos, etc.) que se derivan del uso de los dispositivos y plataformas IoT, interfaces hombre-máquina, entornos inteligentes e inmersivos y la transformación digital en el desarrollo de un sistema software.

COM5. Identificar y valorar las propiedades del software de usabilidad, accesibilidad, seguridad, confiabilidad, rendimiento y ética informática, entre otros, y analizar cómo afecta a la calidad de un sistema software.

Habilidades o destrezas

HD03. Aplica los modelos, métodos, técnicas, paradigmas, algoritmos, lenguajes y herramientas más apropiados para la creación, desarrollo o mantenimiento de sistemas software que cumplan con criterios de calidad, usabilidad, robustez, fiabilidad, seguridad, facilidad de implementación y despliegue en las plataformas más actuales.

HD08. Maneja metodologías, técnicas y buenas prácticas para el desarrollo de sistemas software

seguros.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

TEÓRICO

1. Introducción a la seguridad de los sistemas de información.
    - Fundamentos de seguridad y privacidad de la información.
    - Cumplimiento legal y regulatorio.
    - Etapas en el ciclo de vida de la protección de los sistemas software: Prevención, detección, respuesta y análisis.
    - Análisis de las principales amenazas o vulnerabilidades conocidas e implementación de contramedidas.
    - Recomendaciones y buenas prácticas.
    - Gestión de identidades y accesos.
2. Metodologías y técnicas para el desarrollo de software seguro.
    - Metodologías de desarrollo de software.
    - Ciclo de vida del desarrollo de software seguro.
    - Buenas prácticas para el diseño de sistemas software seguros.
    - DevOps y DevSecOps.
3. Aplicación de tecnologías actuales en seguridad.
    - Introducción a Blockchain y DLT (Distributed Ledger Technology).
    - Taxonomía del Blockchain: Amenazas y vulnerabilidades.
    - Principales arquitecturas de Blockchain y DLT.
    - Blockchain para la seguridad y la privacidad.
    - Hacia la quinta generación de DLT: Blockchain cuántica.

---

1. Introduction to information systems security.
    - Fundamentals of information security and privacy.
    - Legal and regulatory compliance.
    - Stages in the software systems protection lifecycle: Prevention, detection, response, and analysis.
    - Analysis of major known threats or vulnerabilities and implementation of countermeasures.
    - Recommendations and best practices.
    - Identity and access management.
2. Methodologies and techniques for secure software development.
    - Software development methodologies.
    - Secure software development lifecycle.
    - Best practices for designing secure software systems.
    - DevOps and DevSecOps.
3. Application of current technologies in security.
    - Introduction to Blockchain and DLT (Distributed Ledger Technology).
    - Taxonomy of Blockchain: Threats and vulnerabilities.
    - Main Blockchain and DLT architectures.
    - Blockchain for security and privacy.
    - Towards the fifth generation of DLT: Quantum Blockchain.

PRÁCTICO

1. Análisis de amenazas comunes en entornos Web: Uso de frameworks de desarrollo para evitarlas.
2. ⊠Detección automatizada de amenazas de seguridad durante el proceso de desarrollo.
3. Puesta en práctica de DevSecOps mediante Amazon Web Services (AWS).
4. Aplicación de Blockchain y DLT a la seguridad y privacidad de los sistemas software.

---

1. Analysis of common threats in Web environments: Use of development frameworks to avoid them.
2. Automated detection of security threats during the development process.
3. Implementation of DevSecOps using Amazon Web Services (AWS).
4. Application of Blockchain and DLT to the security and privacy of software systems.

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

- Adkins, H., Beyer, B., Blankinship, P., Lewandowski, P., Oprea, A., & Stubblefield, A. (2020). Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems. O'Reilly Media.
- Bergh Johnsson, D., Deogun, D., & Sawano, D. (2019). Secure by Design. Manning Publications.
- Maleh, Y., Shojafar, M., Alazab, M., & Romdhani, I. (2020). Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications. CRC Press.
- Tran, D. A., Thai, M. T., & Krishnamachari, B. (2022). Handbook on Blockchain. Springer.
- Wilson, G. (2020). DevSecOps: A leader's guide to producing secure software without compromising flow, feedback and continuous improvement. Rethink Press.

BIBLIOGRAFÍA COMPLEMENTARIA

- ACISSI, Bancal, D., Ebel, F., Vicogne, F., Fortunato, G., Beirnaert-Huvelle, J., Hennechart, J., Clarhaut, J., Schalkwijk, L., Raultré, R., Dubourg, R., Crocfer, R., Lasson, S. (2022). Seguridad informática - Ethical Hacking: Conocer el ataque para una mejor defensa (5ª edición). Ediciones ENI.
- Bird, J. (2016). DevSecOps: Securing Software through Continuous Delivery. O'Reilly.
- Chilamkurti, N., Poongodi, T., & Balusamy, B. (2021). Blockchain, Internet of Things, and Artificial Intelligence. CRC Press.
- Kim, G., Humble, J., Debois, P., & Willis, J. (2021). The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations (Second Edition). IT Revolution Press.
- McGraw, G. (2018). Software Security: Building Security In. Addison-Wesley Professional.
- Mougayar, W. (2018). La tecnología Blockchain en los negocios: Perspectivas, práctica y aplicación en Internet. Anaya Multimedia.
- Peng, S. (2022). Blockchain for Big Data: AI, IoT, and Cloud perspectives. CRC Press.
- Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice. Pearson.
- Vehent, J. (2018). Securing DevOps: Security in the Cloud. Manning Publications.

ENLACES RECOMENDADOS

Como apoyo a la enseñanza y aprendizaje de esta asignatura, se usará la **Plataforma de Recursos de Apoyo a la Docencia (PRADO)** de la Universidad de Granada: https://prado.ugr.es.

Se recomienda además la lectura de los siguientes contenidos Web:

- https://www.devsecops.org
- https://aws.amazon.com/es/what-is/devsecops/
- https://aws.amazon.com/es/blogs/devops/building-end-to-end-aws-devsecops-ci-cd-pipeline-with-open-source-sca-sast-and-dast-tools/
- https://www.ibm.com/topics/blockchain

EVALUACIÓN (instrumentos de evaluación, criterios de evaluación y porcentaje sobre la calificación final)

EVALUACIÓN ORDINARIA

El artículo 18 de la Normativa de Evaluación y Calificación de los Estudiantes de la Universidad de Granada establece que la convocatoria ordinaria estará basada preferentemente en la evaluación continua del estudiante, excepto para quienes se les haya reconocido el derecho de evaluación única final.

Se realizará una evaluación continua del trabajo del estudiante, valorando tanto los conocimientos adquiridos como las competencias alcanzadas.

Todas las actividades solicitadas por el profesorado de esta asignatura tendrán un **carácter obligatorio**, salvo que se indique lo contrario.

Modalidad presencial:

Para la evaluación en modalidad presencial se tendrán en cuenta los siguientes sistemas de evaluación, indicándose entre paréntesis el rango del porcentaje con respecto a la calificación final del estudiante.

SE1. Actividades realizadas durante el desarrollo del curso mediante la entrega de ejercicios, trabajos, informes, a través de la plataforma docente (55%).

SE2. Actividades realizadas después de finalizar el curso mediante la entrega de ejercicios, trabajos, informes, a través de la plataforma docente (30%).

SE5. Asistencia y participación activa (15%)

Se pedirá la entrega en tiempo y forma de las actividades propuestas a través de la plataforma PRADO.

Modalidad virtual:

Para la evaluación en modalidad virtual se tendrán en cuenta los siguientes sistemas de evaluación, indicándose entre paréntesis el rango del porcentaje con respecto a la calificación

final del estudiante.

SE1. Actividades realizadas durante el desarrollo del curso mediante la entrega de ejercicios, trabajos, informes, a través de la plataforma docente (55%).

SE2. Actividades realizadas después de finalizar el curso mediante la entrega de ejercicios, trabajos, informes, a través de la plataforma docente (30%).

SE6. Participación activa en foros de debate o de recogida de información (15%).

Se pedirá la entrega en tiempo y forma de las actividades propuestas a través de la plataforma PRADO.

EVALUACIÓN EXTRAORDINARIA

El artículo 19 de la Normativa de Evaluación y Calificación de los Estudiantes de la Universidad de Granada establece que los estudiantes que no hayan superado la asignatura en la convocatoria ordinaria dispondrán de una convocatoria extraordinaria. A ella podrán concurrir todos los estudiantes, con independencia de haber seguido o no un proceso de evaluación continua. De esta forma, el estudiante que no haya realizado la evaluación continua tendrá la posibilidad de obtener el 100% de la calificación final.

La evaluación en tal caso consistirá en la realización de una prueba y/o trabajo, y/o las actividades propuestas en la evaluación continua.

EVALUACIÓN ÚNICA FINAL

El artículo 8 de la Normativa de Evaluación y Calificación de los Estudiantes de la Universidad de Granada establece que podrá acogerse a la evaluación única final cualquier estudiante que no pueda cumplir con el método de evaluación continua por causas justificadas.

Para acogerse a la evaluación única final, el estudiante, en las dos primeras semanas de impartición de la asignatura o en las dos semanas siguientes a su matriculación, si ésta se ha producido con posterioridad al inicio de las clases o por causas sobrevenidas, lo solicitará, a través del procedimiento electrónico, a la Coordinación del Máster, quien dará traslado al profesorado correspondiente, alegando y acreditando las razones que le asisten para no poder seguir el sistema de evaluación continua.

La evaluación en tal caso consistirá en la realización de una prueba y/o trabajo, y/o las actividades propuestas en la evaluación continua.

INFORMACIÓN ADICIONAL

Siguiendo las indicaciones recogidas en el artículo 15 de la Normativa de Evaluación y de Calificación de la Universidad de Granada sobre la originalidad de los trabajos presentados por los estudiantes, se informa de lo siguiente:

1. La Universidad de Granada fomentará el respeto a la propiedad intelectual y transmitirá a los estudiantes que el plagio es una práctica contraria a los principios que rigen la formación universitaria. Para ello, procederá a reconocer la autoría de los trabajos y su protección, de acuerdo con la propiedad intelectual, según establezca la legislación vigente.

2. El plagio, entendido como la presentación de un trabajo u obra hecho por otra persona como propio o la copia de textos sin citar su procedencia y dándolos como de elaboración propia, conllevará automáticamente la calificación numérica de cero en la asignatura en la que se hubiera detectado, independientemente del resto de las calificaciones que el estudiante hubiera obtenido. Esta consecuencia debe entenderse sin perjuicio de las responsabilidades disciplinarias en las que pudieran incurrir los estudiantes que plagien.

3. Los trabajos y materiales entregados por parte de los estudiantes tendrán que ir firmados con una declaración explícita en la que se asume la originalidad del trabajo, entendida en el sentido de que no ha utilizado fuentes sin citarlas debidamente.

Información de interés para estudiantado con discapacidad y/o Necesidades Específicas de Apoyo Educativo (NEAE): Gestión de servicios y apoyos (https://ve.ugr.es/servicios/atencion-social/estudiantes-con-discapacidad).