Arquitecturas Seguras

Curso Académico: (2023 / 2024) **Fecha de revisión: 02-05-2023**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: PEREZ MARTINEZ, ALFONSO DE JESUS

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

En esta asignatura se requiere que los estudiantes se manejen cómodamente en entornos Unix y tengan conocimientos de infraestructuras de clave pública, asignatura de Protección de datos.

OBJETIVOS

Al finalizar la asignatura, los alumnos deben adquirir las siguientes competencias generales y específicas:

- Capacidad de analizar la arquitectura de un sistema de información desde el punto de vista de seguridad.

- Capacidad para concebir y diseñar la arquitectura de un sistema de información para que cumpla unos determinados requisitos de seguridad.

- Capacidad para aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto, que minimice los riesgos y proporcione protección contra ataques, especialmente DDoS.

- Capacidad para aprender los procedimientos y principios para gestionar información clasificada.

- Capacidad para 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.

- Capacidad para 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.

- Capacidad para continuar estudiando de manera autónoma.

RESULTADOS DE APRENDIZAJE
Esta asignatura contribuye a los siguientes resultados de aprendizaje:

Dado un sistema con unos requisitos de seguridad establecidos, proponer mecanismos y protocolos necesarios para proporcionar algunos de los servicios básicos de seguridad: autenticación, autorización, privacidad y control de acceso. Dar una medida de su eficacia y limitaciones.

Evaluar la arquitectura de seguridad de un sistema vulnerable dado y proponer mejoras.

Diseñar y evaluar medidas apropiadas para la identificación y autenticación de usuarios, así como la gestión de las identidades y las autorizaciones asociadas.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Esta asignatura profundiza en aspectos relacionados con el diseño de arquitecturas que minimicen los riesgos de seguridad y proporcionen tolerancia frente a ataques. Se cubren también los principios, procedimientos y sistemas para el manejo de información clasificada, así como elementos de seguridad física.

El programa de la asignatura es el siguiente:

1. Introducción a las arquitecturas seguras
1.1. Motivación y casos prácticos

1.2. Principios generales de seguridad en el diseño y despliegue
1.3. Seguridad en arquitectura de "Computación en la Nube"
1.3. Seguridad en arquitectura y aplicaciones nativas de "Computación en la Nube"

2. Autorización
2.1. Modelos de control de acceso tradicionales: DAC, MAC y RBAC
2.2. Modelos de control de acceso recientes: ABAC
2.3. Arquitectura y lenguajes de control de acceso e identidad (IAM): XACML/SAML

3. Tolerancia frente a ataques
3.1. Generalidades y ataques de DoS
3.2. Mecanismos de protección frente a ataques de DDoS
3.3. Sistemas de respaldo y recuperación

4. Sistemas de seguridad multinivel y multilateral
4.1. Clasificación de la información
4.2. Principios y procedimientos de manejo de información clasificada
4.3. Sistemas MLS: Ejemplos y consideraciones prácticas

5. Seguridad Física
5.1. Seguridad frente a las emanaciones. TEMPEST
5.2. Sistemas hardware resistentes a intrusiones

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

Actividades Formativas:

Clase teórica
Clases prácticas
Clases teórico prácticas
Prácticas de laboratorio
Tutorías
Trabajo en grupo
Trabajo individual del estudiante

La metodología docente constará de:

- Clases magistrales: exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.

- Sesiones prácticas y laboratorio: realización de actividades complementarias para ampliar y consolidar los conocimientos de la asignatura. Dichas actividades constan de: problemas, discusiones de casos prácticos y/o prácticas en ordenadores con herramientas útiles para el despliegue de sistemas seguros.

-Elaboración y presentación de trabajos por parte de los alumnos, tanto individuales como en grupo.

SISTEMA DE EVALUACIÓN

El sistema de evaluación se basa en la realización de un trabajo y participación durante el curso, además de un examen final. Concretamente, la evaluación de la asignatura se desglosa en:

1) Trabajo y participación (60%):

1.1) Realización de un trabajo sobre arquitecturas seguras, incluyendo la preparación, exposición y defensa de una presentación técnica

1.2) Trabajos sobre laboratorios guiados relacionados con gestión remota y una arquitectura de identidad y control de acceso y autorización en Linux

2) Examen Final (40%). Examen individual.

Además, se valora la participación por parte de los estudiantes resolviendo problemas, haciendo ejercicios prácticas de demostración, formulando preguntas, etc.

En caso de suspender la asignatura, la evaluación en convocatoria extraordinaria se realiza de la misma forma que la ordinaria: 40% examen, 60% trabajo/participación, para la cual el alumno deberá repetir las partes suspensas.

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60

BIBLIOGRAFÍA BÁSICA

- Bhavani Thuraisingham Developing and Securing the Cloud, Auerbach Publications, 2013
- Dieter Gollmann. Computer Security., John Wiley & Sons., 2011
- Liz Rice, Michael Hausenblas Kubernetes Security, O'Reilly Media, Inc, 2018
- Sam Bishop. Computer Security: Art and Science., Addison- Wesley Professional., 2003
- Sam Newman. Building Microservices., O'Reilly Media, Inc., 2015

BIBLIOGRAFÍA COMPLEMENTARIA

- Fran Ramírez, Elías Grande y Rafael Troncoso. Docker: SecDevOps., 0xWord., 2018
- Guy Podjarny Cloud Native Application Security, O'Reilly Media, Inc., June 2021
- Stephane Jourdan, Pierre Pomes. Infrastructure as Code (IAC) Cookbook., PACKT., 2017
- William Stallings and Lawrie Brown. Computer Security: principles and practice., Pearson Education., 2008