Escuela Superior de Ingeniería
Universidad de Cádiz

Avenida de la Universidad de Cádiz, nº 10
CP 11519, Puerto Real (Cádiz).

| FICHA DE LA ASIGNATURA CRIPTOGRAFÍA APLICADA Y SEGURIDAD EN SOFTWARE DE SISTEMAS | | | |
|---|---|---|---|
| **CARÁCTER:** | **Obligatorio** | **LENGUA/S EN LA/S QUE SE IMPARTE:** | **Español** |
| **ECTS:** | **6** | **CUATRIMESTRE** | **PRIMERO** |
| **Asignatura de la MATERIA SEGURIDAD EN SISTEMAS** | | | |
| **PROFESORES QUE IMPARTEN LA ASIGNATURA** | | | |
| **Juan José Domínguez Jiménez (coordinador)**<br>**Juan Manuel Dodero Beardo**<br>**Manuel Palomo Duarte**<br>**Mercedes Rodríguez García** | | | |
| **COMPETENCIAS QUE SE ADQUIEREN:** *(indicar código)* | | | |
| **Comp. Básicas** | **Comp. Generales** | **Comp. Específicas** | **Comp. Transversales** |
| **CB6 CB7 CB8 CB9**<br>**CB10** | **CG1 CG2 CG3**<br>**CG4 CG5** | **CE6 CE7** | **CT1** |

**RESULTADOS DE APRENDIZAJE:**

Diseñar mecanismos y protocolos necesarios para proporcionar algunos de los servicios básicos de seguridad: autenticación, autorización, privacidad y control de acceso.

Establecer medidas de protección para solventar los problemas de seguridad planteados en sistemas operativos y bases de datos.

**CONTENIDOS:**

Bloque 1: Criptografía
Tema 1: Cifrado y ocultación de información
1.1 Cifrado simétrico
1.2 Cifrado asimétrico
1.3 Esteganografía y marcas al agua digitales (digital watermarking)

Prácticas:

- Aplicación de algoritmos de cifrado simétrico: DES, modos de operación, 2DES, 3DES, AES.
- Aplicación de algoritmos de cifrado asimétrico: RSA, Diffie-Hellman, ECC.
- Esteganografía en imágenes

Tema 2: Autentificación basada en claves
2.1 Funciones unidireccionales

2.2 Autenticación segura
2.3 Salvaguarda segura de claves

Prácticas:
- Funciones hash criptográficas
- Códigos de Autenticación de Mensajes (MAC)

Tema 3: Firma digital y DNIe
3.1 Estándares de firma digital
3.2 Certificados digitales e infraestructuras de clave pública
3.3 DNIe
Prácticas:
- Autoridades de confianza (CA)
- Infraestructuras de clave pública (PKI)

Bloque 2: Seguridad en software de sistemas
Tema 4: Seguridad en sistemas operativos
4.1 Seguridad y protección
4.2 Amenazas a la seguridad y contramedidas
4.3 Principios de diseño para la seguridad
4.3.1 Evitar pérdida de datos
4.3.2 Controlar la confidencialidad de los datos
4.3.3 Controlar el acceso a los datos y a los recursos
4.4 Mecanismos de protección

Tema 5: Seguridad en bases de datos
5.1 El problema de la seguridad en bases de datos
5.2 Control de acceso
5.3 Otros aspectos de seguridad: auditoría y cifrado
5.4 Mantenimiento de la privacidad
5.5 Vulnerabilidades de Bases de de Datos
5.6 Retos en la seguridad de las Bases de Datos
5.7 Data-Driven security
5.8 Seguridad en CMS
Prácticas
- Seguridad de BBDD
- Seguridad en CMS

Tema 6: Seguridad en sistemas abiertos
6.1. Interoperabilidad y estándares: esquemas, metadatos, ontologías
6.2. Data cleansing: data wrangling, herramientas
6.3. Seguridad en datos abiertos: justificación, enlazado y guías
6.4. Data preservation

6.5. Seguridad en open source: certificaciones y sistemas
Prácticas:
- Data cleansing
- Data preservation

**OBSERVACIONES / REQUISITOS PREVIOS:**
Algunas de las actividades pueden realizarse en inglés

| | Id de la Actividad Formativa | Nº de horas | Presencialidad (%) |
|---|---|---|---|
| **ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:** | Clases de teoría | 8 | 100% |
| | Clases de prácticas | 8 | 100% |
| | Clases teórico prácticas | | |
| | Seminarios y conferencias | | |
| | Actividades académicas no presenciales | 96 | 0% |
| | Evaluación | 4 | 100% |

**METODOLOGÍAS DOCENTES:**

Lección magistral expositiva

Resolución de problemas y casos prácticos

Prácticas de ordenador

Realización de trabajos

**SISTEMAS DE EVALUACIÓN DE ADQUISICIÓN DE COMPETENCIAS:**

| Denominación Sistema Evaluación | Ponderación Mínima | Ponderación Máxima |
|---|---|---|
| Prácticas de informática | 10% | 30% |
| Participación y trabajo realizado en actividades formativas | 0% | 20% |
| Pruebas escritas u orales | 40% | 70% |

**BIBLIOGRAFÍA RECOMENDADA:**

Bruce Schneider Applied Cryptography 2 ed, Wiley. 1996 ISBN: 0-471-11709-9

Paar, Christof, Jan Pelzl Understanding Cryptography: A Textbook for Students and Practitioners Springer. 2009 ISBN: 978-3-642-04100-6

David G. Hill. Data Protection: Governance, Risk Management, and Compliance. CRC Press. 2009. ISBN: 978-14-398-0692-0

Jordi Serra, Daniel Lerch Esteganografía y estegoanálisis 0xWord, 2014 ISBN: 978-84-617-0021-9

Data-Driven Security: Analysis, Visualization and Dashboards J. Jacobs, B. Rudis John Wiley & Sons, 2014

Ron Ben Natan, Implementing Database Security and Auditing, 1st Edition, Digital Press, 2005.

David Litchfield, Chris Anley, John Heasman, Bill Grindlay, The Database Hacker's Handbook: Defending Database Servers, 1st Edition, 2005.

Open Source Systems Security Certification E. Damiani, C. A. Ardagna, N. El Ioini Springer, 2009

Linux Server Security, 2ª edición Michael D. Bauer (2005), O'Reilly Media, 2005

Operating System Security. Synthesis Lectures on Information Security, Privacy, and Trust.

Trent Jaeger. The Pennsylvania State University doi:10.2200/S00126ED1V01Y200808SPT001

Linked data: evolving the web into a global data space Morgan & Claypool, 2011

The Tao of Network Security Monitoring: Beyond Intrusion Detection Richard Bejtlich Addison-Wesley, 2004

Science Data Preservation: Implementation and Why It Is Important. NASA, 2013. Autor Steven J. Kempler

Complete Guide to Anonymous Torrent Downloading and File-sharing: A practical, step-by-step guide on how to protect your Internet privacy and anonymity both online and offline while torrenting. Nerel Publications, 2013.

The Complete Book of Data Anonymization: From Planning to Implementation. CRC Press 2013. Autor Balaji Raghunathan

Fundamentos de Sistemas de Bases de Datos, ADDISON WESLEY; Edición: 5, 2007, Elmasri & Navathe