



Guía Docente

| Datos Identificativos | | | | | 2012/13 |
|-----------------------|--|----------|--------------------|----------------------|-----------|
| Asignatura (*) | Seguridade en Sistemas de Información | | | Código | 614451122 |
| Titulación | | | | | |
| Descritores | | | | | |
| Ciclo | Período | Curso | Tipo | Créditos | |
| Mestrado Oficial | 2º cuatrimestre | Primeiro | Obrigatoria | 4 | |
| Idioma | Castelán | | | | |
| Prerrequisitos | | | | | |
| Departamento | Tecnoloxías da Información e as Comunicaci3ns | | | | |
| Coordinaci3n | Gestal Pose, Marcos | | Correo electr3nico | marcos.gestal@udc.es | |
| Profesorado | Gestal Pose, Marcos | | Correo electr3nico | marcos.gestal@udc.es | |
| Web | campusvirtual.udc.es | | | | |
| Descrici3n xeral | <p>La seguridad en los sistemas de informaci3n es crucial en todos y cada uno de los servicios ofertados por la denominada sociedad de la informaci3n. Incluso en este 3mbito, todav3a en desarrollo, los requisitos de seguridad cambian a un ritmo vertiginoso. Puesto que cada vez m3s informaci3n est3 accesible, cada vez se requieren controles de seguridad m3s estrictos. El avance tecnol3gico en este caso funciona de catalizador en ambas direcciones: por un lado favorece el acceso a nuevos tipos y a mayor cantidad de informaci3n (lo que requiere un aumento de los controles de seguridad) y por otro lado posibilita la implantaci3n de mecanismos de seguridad m3s refinados (que posibilitan el acceso seguro a nuevos tipos de informaci3n).</p> <p>La asignatura est3 planteada para proporcionar al alumno el conocimiento necesario de los conceptos b3sicos y t3cnicas empleadas para la protecci3n de los sistemas de informaci3n, desde el punto de vista f3sico, l3gico, administrativo y legal. Estos conceptos b3sicos incluir3n, como paso de inicio, la evoluci3n de los diferentes m3todos y algoritmos de cifrado. Debido al enorme auge de los diversos medios electr3nicos de intercambio de informaci3n (correo electr3nico, p3ginas web, e-commerce, firma digital, etc.) un aspecto fundamental cuando se trabaja en este 3mbito ser3 tener la formaci3n suficiente en la seguridad de este tipo de sistemas. Para el correcto funcionamiento de los servicios referidos se exige la existencia de una infraestructura (redes de comunicaciones y sistemas operativos) que funcione de modo seguro y confiable. Por lo tanto ser3 necesario conocer los aspectos fundamentales de los componentes, protocolos de funcionamiento, configuraci3n, etc. de dicha infraestructura.</p> <p>Dichos conocimientos ser3n los que le permitan entender y solucionar los riesgos actuales, y los que inevitablemente surgir3n en el futuro, que afectan a todo sistema de informaci3n.</p> <p>Objetivos:</p> <ul style="list-style-type: none">- Familiarizarse con el proceso de la seguridad- Identificar los riesgos de los sistemas de informaci3n- Conocer distintos mecanismos para dotar de seguridad a un sistema de informaci3n- Comprender los conceptos fundamentales de la criptograf3a- Entender qu3 es, c3mo se define y c3mo se aplica una pol3tica de seguridad | | | | |

Competencias da titulaci3n

| C3digo | Competencias da titulaci3n |
|--------|----------------------------|
|--------|----------------------------|

Resultados da aprendizaxe

| Competencias de materia (Resultados de aprendizaxe) | Competencias da titulaci3n |
|---|----------------------------|
|---|----------------------------|



| | | | |
|---|---|--|--------------------------|
| Resumir los fundamentos de los criptosistemas | AP5 AP6 AP8 | BP1 BP8 | CM1 |
| Definir los riesgos y vulnerabilidades de un sistema de información | AP1 AP5 AP6 AP8 AP9 | BP1 BP3 BP4 BP5 BP6 BP8 BP11 | CM1 |
| Analizar los nuevos avances en seguridad y sus repercusiones | AP6 AP8 AP9 AP10 | BP3 BP8 BP11 BP15 | CM1 CM2 CM8 |
| Utilizar las herramientas de seguridad | AP6 | BP4 BP5 BP10 | CM3 |
| Organizar la seguridad de un sistema de información | AP3 AP7 AP8 | BP4 BP5 BP6 BP7 | CM3 CM6 |
| Expresar de forma clara y efectiva la necesidad, implantación, ventajas y desventajas de las medidas de seguridad | AP6 | BP1 BP3 BP8 | CM6 CM7 CM8 |
| Asumir la existencia de vulnerabilidades en los sistemas de información e intentar su minimización | AP6 | BP5 BP6 BP8 | CM3 CM4 CM7 |
| Colaborar con otros profesionales (administradores de sistemas, redes, bases de datos, aplicaciones, etc.) en la puesta en marcha y mantenimiento de las medidas de seguridad | AP2 AP3 AP4 AP6 AP9 AP10 | BP1 BP2 BP4 BP5 BP6 BP7 BP8 BP9 | CM3 CM4 CM6 CM7 |

| Contidos | |
|----------------------------------|--|
| Temas | Subtemas |
| Fundamentos | 1.- Fundamentos de Teoría de la Seguridad 2.- Seguridad física y lógica |
| Criptografía | 3.- Sistemas criptográficos clásicos 4.- Sistemas criptográficos de clave secreta 5.- Sistemas criptográficos de clave pública 6.- Firma digital |
| Seguridad en Sistemas Operativos | 7.- Seguridad en sistemas Linux 8.- Seguridad en sistemas Windows |
| Seguridad en Redes | 9.- Fundamentos de Redes de Comunicaciones. 10.- Elementos de seguridad en redes de comunicaciones: firewall, filtros, proxy 11.- Vulnerabilidades y Seguridad en Internet: WWW, correo electrónico. |



| | |
|---------------------|---|
| Conceptos Avanzados | 12.- Esteganografía, criptografía visual 13.- Análisis forense |
| Temario Prácticas | 1. Políticas de Seguridad 2. Criptografía y criptoanálisis clásicos 3. Configuración seguridad y detección de intrusos en sistemas operativos 4. PGP 5. Configuración de seguridad y detección de intrusos en servidores web 6. Análisis forense |

| Planificación | | | |
|---------------------------------------|-------------------|---|--------------|
| Metodoloxías / probas | Horas presenciais | Horas non presenciais / traballo autónomo | Horas totais |
| Sesión maxistral | 6 | 9 | 15 |
| Prácticas de laboratorio | 18 | 9 | 27 |
| Traballos tutelados | 8 | 20 | 28 |
| Presentación oral | 10 | 10 | 20 |
| Proba mixta | 2 | 2 | 4 |
| Eventos científicos e/ou divulgativos | 2 | 0 | 2 |
| Atención personalizada | 4 | 0 | 4 |

*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado

| Metodoloxías | |
|---------------------------------------|---|
| Metodoloxías | Descrición |
| Sesión maxistral | Introducción conceptos y aspectos clave de cada uno de los temas |
| Prácticas de laboratorio | Búsqueda información para los trabajos tutelados |
| Traballos tutelados | Trabajos académicos relativos al contenido teórico de la asignatura |
| Presentación oral | Presentación trabajos dirigidos |
| Proba mixta | Realización examen. |
| Eventos científicos e/ou divulgativos | Asistencia a eventos de interés |

| Atención personalizada | |
|--------------------------|---|
| Metodoloxías | Descrición |
| Traballos tutelados | Resolución de dudas. |
| Prácticas de laboratorio | Tutorización personalizada trabajos individuales. |

| Avaliación | | |
|--------------------------|--|---------------|
| Metodoloxías | Descrición | Cualificación |
| Traballos tutelados | Realización de trabajos tutelados: Criterios evaluación: calidad trabajos y presentaciones, participación activa en las defensas de los compañeros, actitud | 45 |
| Prácticas de laboratorio | Realización de prácticas Criterios de evaluación: Aprovechamiento horas laboratorio, defensa de la práctica | 35 |



| | | |
|------------------|---|----|
| Sesión maxistral | Asimilación de Conceptos Teóricos, relativos a los bloques de teoría, prácticas de laboratorio y trabajos tutelados). Nota mínima exigida: 5 | 20 |
| Outros | | |

Observacións avaliación

El proceso de evaluación será continuo a lo largo de la realización de la materia. La evaluación se compondrá de varios apartados distintos: asimilación conceptos teóricos, realización de prácticas y exposición de trabajos que se valorarán según la ponderación indicada a continuación.

La nota final de la asignatura vendrá determinada por una evaluación ponderada de los tres bloques que forman parte de ella:

- 1) El 45% de la nota vendrá dada por la realización de los trabajos tutelados. Los criterios a valorar serán la calidad de los trabajos presentados, la claridad y calidad de las presentaciones realizada, la participación activa en las defensas de los trabajos de los compañeros o la actitud
- 2) El 35% de la nota vendrá dada por las prácticas de laboratorio. Se perseguirá realizar una evaluación continua, o en todo caso, valorar el aprovechamiento de las horas de laboratorio y la defensa de las prácticas realizadas.
- 3) El 20% restante de la nota vendrá dado por la realización de un examen teórico. En este examen, tipo test, se valorará la asimilación de los contenidos de la asignatura, mediante preguntas relativas a los bloques de teoría, práctica y trabajos tutelados. Será necesaria una nota mínima de un 5 en este examen para poder aprobar la asignatura.

Fontes de información

| | |
|------------------------------------|--|
| Bibliografía básica | <ul style="list-style-type: none">- Jorge Ramió (1999). Aplicaciones Criptográficas. UPM- S. Harris (2010). CISSP All in one. 5ª Edición. Mc-Graw Hill- W. Stallings (2004). Fundamentos de Seguridad en Redes. Aplicaciones y Estándares. 2ª Edición. Pearson Educación- M. Mackrill, C. Nowell, K. Stopford, C. Trautwein (2011). Official ISC2 Guide to the SSCP CBK. 2ª Edición. Ed. Harold F. Tripton |
| Bibliografía complementaria | <ul style="list-style-type: none">- Manuel J. Lucena (). Critpografía y seguridad en Computadores. http://www.di.ujaen.es/~mlucena- Simson Garfinkel, Gene Spafford, Alan Schwartz (2003). Practical UNIX and Internet Security, Third Edition. O'Reilly- Information Security Forum (). The Standard of good Practice for Information Security. http://www.isfsecuritystandard.com |

Recomendacións

Materias que se recomienda ter cursado previamente

Materias que se recomienda cursar simultaneamente

Materias que continúan o temario

Observacións



Otros recursos web de interés:

Kriptopolis: www.kriptopolis.com

Criptored: www.criptored.upm.es

PGP : www.pgpi.org

Otros materiales de apoyo:

Se proporcionarán al alumno todas las transparencias empleadas para el desarrollo de las clases, así como referencias bibliográficas en las que pueda profundizar en el estudio de determinados puntos del temario.

(*A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías