



Guía docente				
Datos Identificativos				2021/22
Asignatura (*)	Seguridad en los sistemas Informáticos	Código	614G01079	
Titulación	Grao en Enxeñaría Informática			
Descritores				
Ciclo	Periodo	Curso	Tipo	Créditos
Grado	1º cuatrimestre	Cuarto	Optativa	6
Idioma	Castellano			
Modalidad docente	Híbrida			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputación			
Coordinador/a	Vázquez Naya, José Manuel	Correo electrónico	jose.manuel.vazquez.naya@udc.es	
Profesorado	Vázquez Naya, José Manuel	Correo electrónico	jose.manuel.vazquez.naya@udc.es	
Web	<a href="https://campusvirtual.udc.gal">https://campusvirtual.udc.gal</a>			
Descripción general	<p>La seguridad en los sistemas de información es crucial en todos y cada uno de los servicios ofertados por la denominada sociedad de la información. Puesto que cada vez más información está accesible, cada vez se requieren controles de seguridad más estrictos. El avance tecnológico en este caso funciona de catalizador en ambas direcciones: por un lado favorece el acceso a nuevos tipos y a mayor cantidad de información (lo que requiere un aumento de los controles de seguridad) y por otro lado posibilita la implantación de mecanismos de seguridad más refinados (que posibilitan el acceso seguro a nuevos tipos de información).</p> <p>La asignatura está planteada para proporcionar al alumno el conocimiento necesario de los conceptos básicos y técnicas empleadas para la protección de los sistemas de información, desde el punto de vista físico, lógico y administrativo. Estos conceptos básicos incluirán, como paso de inicio, la evolución de los diferentes métodos y algoritmos de cifrado. Debido al enorme auge de los diversos medios electrónicos de intercambio de información (correo electrónico, páginas web, e-commerce, firma digital, etc.) un aspecto fundamental cuando se trabaja en este ámbito será tener la formación 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 será necesario conocer los aspectos fundamentales de los componentes, protocolos de funcionamiento, configuración, etc. de dicha infraestructura. Dichos conocimientos serán los que le permitan entender y solucionar los riesgos actuales, y los que inevitablemente surgirán en el futuro, que afectan a todo sistema de información.</p>			



<b>Plan de contingencia</b>	<p>1. Modificaciones en los contenidos</p> <ul style="list-style-type: none"> <li>- No se realizarán cambios</li> </ul> <p>2. Metodologías</p> <p>*Metodologías docentes que se mantienen</p> <ul style="list-style-type: none"> <li>- Se mantienen las metodologías docentes, con la excepción de que, en lugar de realizarse de manera presencial en el aula, se realizarán con la ayuda de herramientas TIC, como se explica a continuación.</li> </ul> <p>*Metodologías docentes que se modifican</p> <ul style="list-style-type: none"> <li>- Sesión magistral: se impartirá a través de videoconferencia.</li> <li>- Prácticas de laboratorio: Tanto la docencia, como la defensa de las prácticas, cuando proceda, se realizarán a través de videoconferencia.</li> <li>- Prueba objetiva: se realizará a través de Moodle, en combinación con videoconferencia.</li> <li>- Examen de prácticas (segunda oportunidad y convocatoria extraordinaria): se realizará a través de videoconferencia.</li> </ul> <p>3. Mecanismos de atención personalizada al alumnado</p> <ul style="list-style-type: none"> <li>- Correo electrónico: Diariamente. De uso para hacer consultas, y solicitar encuentros virtuales para resolver dudas.</li> <li>- Moodle: Diariamente. Según la necesidad del alumnado.</li> <li>- Teams: Durante las horas programadas de teoría y práctica. También bajo demanda, para resolución de dudas.</li> </ul> <p>4. Modificaciones en la evaluación</p> <ul style="list-style-type: none"> <li>- No se realizarán cambios</li> </ul> <p>*Observaciones de evaluación:</p> <p>Se mantienen las mismas que figuran en la guía docente. A mayores:</p> <ul style="list-style-type: none"> <li>- En caso de que no puedan realizarse presencialmente, se llevarán a cabo según lo indicado en el apartado de "Metodologías".</li> <li>- Si por algún motivo justificado el alumno no pudiera realizar el examen final (prueba objetiva) en el momento establecido, el examen pasará a realizarse la mayor brevedad posible, pasando a ser una prueba oral por videoconferencia.</li> </ul> <p>5. Modificaciones de la bibliografía o webgrafía</p> <p>Ninguna.</p>
-----------------------------	--

Competencias / Resultados del título	
Código	Competencias / Resultados del título
A58	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
B1	Capacidad de resolución de problemas
B3	Capacidad de análisis y síntesis
C3	Utilizar las herramientas básicas de las tecnologías de la información y las comunicaciones (TIC) necesarias para el ejercicio de su profesión y para el aprendizaje a lo largo de su vida.
C6	Valorar críticamente el conocimiento, la tecnología y la información disponible para resolver los problemas con los que deben enfrentarse.

<b>Resultados de aprendizaje</b>
----------------------------------



Resultados de aprendizaje	Competencias / Resultados del título		
	A58	B3	C3 C6
Identificar los fundamentos de los criptosistemas e identificar los mecanismos de seguridad así como su integración en las organizaciones	A58	B3	C3 C6
Definir los riesgos y vulnerabilidades de un sistema de información y su aplicación en entornos reales.	A58	B1	C3 C6
Utilizar herramientas de seguridad	A58	B1	C3
Organizar la seguridad de un sistema de información	A58	B1	C3 C6
Expresar de forma clara y efectiva la necesidad, implantación, ventajas y desventajas de las medidas de seguridad	A58	B3	C3 C6

Contenidos	
Tema	Subtema
Criptología	Sistemas criptográficos clásicos Sistemas criptográficos de clave secreta Sistemas criptográficos de clave pública Firma digital Esteganografía
Seguridad en el correo electrónico	PGP GPG S/MIME
Sistemas de Gestión de Seguridad de la Información	Normativas de Seguridad Estándares de Gestión de la Seguridad de la Información Normas ISO / IEC 27000 Implantación de un SGSI
Análisis de Riesgos y Medidas de Seguridad	Análisis de Riesgos Gestión del Riesgo Medidas de Seguridad
Malware	Virus &quot;Trojans&quot; &quot;Rootkits&quot; &quot;Exploits&quot;
Análisis Forense	Fases del Análisis Forense Herramientas HW y SW
Estudio de casos	Estudio de casos reales de ataques a sistemas de información
Prácticas	Prueba de distintas herramientas de seguridad, relacionadas con los temas de teoría

Planificación				
Metodologías / pruebas	Competencias / Resultados	Horas lectivas (presenciales y virtuales)	Horas trabajo autónomo	Horas totales
Sesión magistral	B3	16	32	48
Prácticas de laboratorio	A58 B1 C3 C6	18	36	54
Trabajos tutelados	A58 B3 C3 C6	10	30	40
Prueba objetiva	A58 B1	1	0	1
Atención personalizada		7	0	7

(\*Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos



## Metodologías

Metodologías	Descrición
Sesión magistral	<p>Clases expositivas de presentación de los conocimientos teóricos de cada uno de los temas.</p> <p>El material utilizado en estas clases estará disponible en la plataforma de formación de la Universidade da Coruña.</p>
Prácticas de laboratorio	<p>Sesiones prácticas en ordenador, en las que se deben resolver una serie de boletines de ejercicios prácticos propuestos por el profesor. Los ejercicios buscan consolidar los conocimientos presentados en las sesiones magistrales y también fomentar el aprendizaje autónomo del alumno. En la resolución de los ejercicios, se utilizarán distintas herramientas de seguridad, con el objetivo de que el alumno las conozca y adquiera destreza en su uso.</p> <p>Algunos ejercicios tienen carácter individual, mientras que otros serán realizados en grupo.</p> <p>Los boletines de ejercicios se publicarán a través de la plataforma de formación de la Universidade da Coruña.</p>
Trabajos tutelados	<p>Trabajos tutelados relativos al contenido de la asignatura, que se realizan en grupos pequeños. El profesor propondrá un listado de temas, relacionados con el temario de la asignatura. Los alumnos deberán escoger un tema y consensuar la estructura del trabajo con el profesor. Finalmente, los alumnos deben realizar una presentación en clase del trabajo realizado.</p> <p>El objetivo de los trabajos es que el alumno profundice en un tema de su interés.</p>
Prueba objetiva	Prueba escrita mediante la que se valorarán los conocimientos y capacidades adquiridos por el alumno.

## Atención personalizada

Metodologías	Descrición
Trabajos tutelados	Resolución de dudas.
Prácticas de laboratorio	Supervisión de los trabajos tutelados.

## Evaluación

Metodologías	Competencias / Resultados	Descrición	Calificación
Prueba objetiva	A58 B1	Al finalizar el cuatrimestre, se realizará una prueba escrita mediante la que se valorarán los conocimientos y capacidades adquiridos por el alumno.	40
Trabajos tutelados	A58 B3 C3 C6	<p>Realización del trabajo tutelado y su presentación en clase.</p> <p>Criterios evaluación: dificultad de la temática, trabajo de búsqueda y selección de material relevante, calidad y cantidad de las fuentes de información seleccionadas, capacidad de síntesis, existencia de componente práctica o realización de pruebas, calidad de la memoria y calidad de la presentación.</p>	30
Prácticas de laboratorio	A58 B1 C3 C6	En el enunciado de cada práctica se especificará la fecha límite para la realización de la misma, así como la metodología de evaluación, que puede ser a través de la entrega de una memoria, de la realización de una prueba en ordenador, o mediante ambas.	30
Otros			

## Observaciones evaluación



## 1. PRIMERA OPORTUNIDAD

Al largo del curso se realizarán una serie de "prácticas de laboratorio" y un "trabajo tutelado", con las características y peso indicados en el cuadro anterior.

Al finalizar el curso se realizará una "prueba objetiva", con las características y peso indicados en el cuadro anterior.

## 2. SEGUNDA OPORTUNIDAD Y OPORTUNIDAD ADELANTADA

Se realizará una "prueba objetiva", con las características y peso indicados en el cuadro anterior.

Las notas de "prácticas de laboratorio" y del "trabajo tutelado" obtenidas en la primera oportunidad, se conserva para el resto de oportunidades de ese curso.

Caso de no tener nota en alguno de estos apartados, y querer optar a ella, el alumno debe contactar con el coordinador de la materia con una antelación mínima de 30 días naturales antes de la fecha del examen.

La nota de "prácticas de laboratorio" podrá recuperarse mediante la realización y defensa de las prácticas que se determinen para la segunda oportunidad (u oportunidad adelantada de diciembre, segundo correspondida).

La nota del "trabajo tutelado" podrá recuperarse mediante la realización y defensa de un trabajo tutelado individual, cuya temática debe ser acordada con el coordinador de la materia.

## 3. CONDICIÓN DE "NO PRESENTADO"

Se considerarán como "no presentados" a los alumnos que no realicen la prueba objetiva.

## 4. ALUMNOS A TIEMPO PARCIAL

Alumnado con reconocimiento de dedicación a tiempo parcial.

Los alumnos que cursen la materia a tiempo parcial deben realizar las mismas pruebas de evaluación que los alumnos que las cursen a tiempo completo, con las siguientes consideraciones:

- En cuanto a la defensa de las prácticas, si el alumno no pudiera asistir a la defensa en el horario de prácticas, se convendrá con él un horario alternativo.

El alumno deberá notificar al coordinador de la materia su condición de estudiante a tiempo parcial tan pronto como le sea reconocida, para que el profesor pueda realizar una correcta planificación de las actividades docentes.

### Fuentes de información

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

### Recomendaciones

#### Asignaturas que se recomienda haber cursado previamente

Legislación y Seguridad Informática/614G01024

Administración de Sistemas Operativos/614G01047

Administración de Redes/614G01048

Administración de Bases de Datos/614G01050

#### Asignaturas que se recomienda cursar simultáneamente

#### Asignaturas que continúan el temario

#### Otros comentarios



(\*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías