Guia docente				
Datos Identificativos				2023/24
Asignatura (*)	Seguridad en los sistemas Informáticos		Código	614G01079
Titulación	Grao en Enxeñaría Informática			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Grado	1º cuatrimestre	Cuarto	Optativa	6
Idioma	Castellano			
Modalidad docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputación			
Coordinador/a	Vázquez Naya, José Manuel	Correo electrónico	jose.manuel.vazquez.naya@udc.es	
Profesorado	Rivera Dourado, Martiño Vázquez Naya, José Manuel	Correo electrónico	martino.rivera.dourado@udc.es jose.manuel.vazquez.naya@udc.es	
Web	https://campusvirtual.udc.gal			
Descripción general	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). 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.			

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.

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias / Resultados del título		
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 de clave secreta - Cifradores de bloque - Cifradores de flujo Sistemas criptográficos de clave pública Técnicas de criptoanálisis Esteganografía Funciones hash Firma digital Certificados digitales Autoridades de certificación Tarjetas inteligentes
Seguridad en el correo electrónico	PGP - GPG S/MIME
Normativas de Seguridad	Estándares de Gestión de la Seguridad de la Información Normas ISO / IEC 27000 Implantación de un SGSI
Malware	Virus "Trojans" "Rootkits" "Exploits"
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	21	42	63
Prácticas de laboratorio	A58 B1 C3 C6	15	30	45
Trabajos tutelados	A58 B3 C3 C6	6	24	30
Prueba objetiva	A58 B1	1	0	1
Atención personalizada		11	0	11
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	**Descripción**
Sesión magistral	Clases expositivas de presentación de los conocimientos teóricos de cada uno de los temas. El material utilizado en estas clases estará disponible en la plataforma de formación de la Universidade da Coruña.

Prácticas de laboratorio	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. Algunos ejercicios tienen carácter individual, mientras que otros serán realizados en grupo. Los boletines de ejercicios se publicarán a través de la plataforma de formación de la Universidade da Coruña.
Trabajos tutelados	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. El objetivo de los trabajos es que el alumno profundice en un tema de su interés.
Prueba objetiva	Prueba escrita mediante la que se valorarán los conocimientos y capacidades adquiridos por el alumno.

Atención personalizada	
Metodologías	**Descripción**
Trabajos tutelados Prácticas de laboratorio Sesión magistral	En la realización de las prácticas de laboratorio y de los trabajos tutelados, se realizará un "Seguimiento continuado" o "Atención personalizada". De modo que, para obtener la máxima nota, será necesario participar de manera activa durante el desarrollo de los mismos. También en la "Sesión Magistral" se realizará un "Seguimiento continuado" o "Atención personalizada". Se plantearán preguntas y retos. Se fomentará el debate en clase. Se valorará la participación activa.

Evaluación			
Metodologías	**Competencias / Resultados**	**Descripción**	**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.	50
Trabajos tutelados	A58 B3 C3 C6	Realización del trabajo tutelado y su presentación en clase. 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. Se realizará un "Seguimiento continuado" o "Atención personalizada". De modo que, para obtener la máxima nota, será necesario participar de manera activa durante el desarrollo de los trabajos tutelados.	20

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. Se realizará un "Seguimiento continuado" o "Atención personalizada". De modo que, para obtener la máxima nota, será necesario participar de manera activa durante el desarrollo de las prácticas.	30
Otros			

Observaciones evaluación

Será necesario obtener como mínimo el 50% de la nota para aprobar la materia. Además, para aprobar la materia será preciso (en cualquier oportunidad) obtener un mínimo de un 40% de la nota en la prueba objetiva. En caso contrario, la nota máxima que se podrá obtener es de 4.5.
La nota de la prueba objetiva NO se conserva en ninguna convocatoria. La nota de "prácticas de laboratorio" y de "trabajos tutelados" se conserva para el resto de oportunidades del curso académico.
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.
La nota de "prácticas de laboratorio" podrá recuperarse mediante la realización de las prácticas que se determinen para la segunda oportunidad (u oportunidad adelantada). La presentación de las prácticas en la convocatoria de segunda oportunidad (u oportunidad adelantada) implica la renuncia a la nota obtenida previamente, si la hubiera.
La nota del "trabajo tutelado" podrá recuperarse mediante la realización de un nuevo trabajo, cuya temática debe ser acordada con el coordinador de la materia. La presentación del trabajo tutelado en la convocatoria de segunda oportunidad (u oportunidad adelantada) implica la renuncia a la nota obtenida en la primera oportunidad, si la hubiera.
Caso de querer recuperar la nota de prácticas de laboratorio o del trabajo tutelado en la convocatoria de segunda oportunidad (u oportunidad adelantada), el alumnado deberá contactar con el coordinador de la materia, con una antelación mínima de 20 días naturales antes de la fecha del examen de la correspondiente convocatoria.
3. CONDICIÓN DE "NO PRESENTADO"
Se considerará como "no presentado" al alumnado que no se presente a ninguna de las actividades evaluables en una convocatoria dada.
4. ALUMNADO A TIEMPO PARCIAL O CON DISPENSA ACADÉMICA DE EXENCIÓN DE DOCENCIA
El alumnado que curse la materia a tiempo parcial o con dispensa académica de exención de docencia debe realizar las mismas pruebas de evaluación que el alumnado que la curse a tiempo completo, con las siguientes consideraciones:
- En cuanto a la realización de las prácticas, podrá realizarlas de manera individual. En caso de que no pudiera asistir a la defensa en el horario de prácticas, se convendrá un horario alternativo.
- En cuanto a la realización del trabajo tutelado, podrá realizarlo de manera individual. En caso de que no pudiera asistir a la presentación del mismo en el horario de prácticas, se convendrá un horario alternativo.
El alumnado deberá notificar al coordinador de la materia su condición de estudiante a tiempo parcial o con dispensa académica de exención de docencia tan pronto como le sea reconocida, para que este pueda realizar una correcta planificación de las actividades docentes.
5. COPIA Y/O PLAGIO
A realización fraudulenta de las pruebas o actividades de evaluación, una vez comprobada, implicará directamente la calificación de suspenso en la convocatoria en que se cometa: el/la estudiante será calificado con "suspenso" (nota numérica 0) en la convocatoria correspondiente del curso académico, tanto se la comisión de la falta se produce en la primera oportunidad como en la segunda. Para esto, se procederá a modificar su calificación en el acta de primera oportunidad, si fuera necesario.

Fuentes de información

Básica	- Stallings, W. (2011). Cryptography and Network Security: Principles and Practice (Fifth ed.). Prentice Hall - Jorge Ramió (1999). Aplicaciones Criptográficas. UPM - M. Mackrill, C. Nowell, K. Stopford, C. Trautwein (2011). Official ISC2 Guide to the SSCP CBK. 2ª Edición. Ed. Harold F. Tripton - S. Harris (2010). CISSP All in one. 5ª Edición. Mc-Graw Hill
Complementária	- Schneier, B. (2007). Applied cryptography: protocols, algorithms, and source code in C. Wiley-India - Simson Garfinkel, Gene Spafford, Alan Schwartz (2003). Practical UNIX and Internet Security, Third Edition. O'Reilly - Manuel J. Lucena (). Critpografía y seguridad en Computadores. http://wwwdi.ujaen.es/~mlucena - Information Security Forum (). The Standard of good Practice for Information Security. http://www.isfsecuritystandard.com

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