Guía Docente: Tecnologías Aplicadas a la Gestión de la Seguridad

DATOS GENERALES	
Facultad	Facultad de Criminología
Titulación	Grado en Ciencias de la Seguridad
Plan de estudios	2016
Materia	Informática
Carácter	Obligatorio
Período de impartición	Tercer Trimestre
Curso	Primero
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No existen requisitos previos para esta asignatura.

DATOS DEL PROFESORADO			
Profesor Responsable	Javier Martín Porras	**Correo electrónico**	javier.martin.porras@ui1.es
Área	Lenguajes y Sistemas Informáticos	**Facultad**	Facultad de Criminología
Perfil Profesional 2.0	Es ingeniero Superior en Informática y Doctor en Ingeniería Informática. Es Profesor en varios grados de la Universidad Isabel I, y ejerce como perito en "Laboratorio Pericial Forense" en Alicante. Consultor Internacional de la Oficina de Naciones Unidas contra la Droga y el Delito. Laboratorio Pericial Forense		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Aplicación de las TIC a la Práctica Profesional • Ciberseguridad en Redes y Sistemas • Tecnologías Aplicadas a la Gestión de la Seguridad
Contexto y sentido de la asignatura en la titulación y perfil profesional	• El campo de la seguridad de la información ha crecido y evolucionado considerablemente en los últimos años convirtiéndose en un área critica en empresas, organizaciones y gobiernos. • Vulnerabilidades, amenazas y protocolos de seguridad son grandes desconocidos para el público general, pero deben de ser conocidos en profundidad por los profesionales de todas las áreas de la seguridad. • Esta asignatura pretende profundizar en los sistemas y redes de comunicación para seguridad y emergencias, así como en la protección de Infraestructuras críticas. • Esta asignatura esta especialmente relacionada con la aplicación de las TIC´s y con las tecnologias aplicadas a la gestión de la seguridad.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CB01: Poseer y comprender conocimientos en un área de estudio que parte de la base de la Educación Secundaria General, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio. • CB03: Reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética. • CB04: Transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. • CB05: Desarrollar aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. • CG01: Conocer, saber organizar y planificar los recursos individuales y colectivos disponibles para el ejercicio, en sus distintas modalidades, de la profesión. • CG02: Capacidad para asesorar a terceros en cuestiones concretas y específicas que solo la especialización en una materia puede otorgar. • CG03: Capacidad de gestión de la información, de redacción de informes y/o artículos de investigación con una actitud creativa e innovadora y mediante el empleo de una correcta técnica de investigación. • CG04: Resolución de problemas en materias relativas a la seguridad. • CG05: Motivación por la calidad. • CU04: Utilizar las tecnologías de la información y la comunicación (TIC) para poner en marcha procesos de trabajo ajustados a las necesidades de la sociedad actual. • CU05: Realizar investigaciones basándose en métodos científicos que promuevan un avance en la profesión. • CU06: Aprender a trabajar individualmente de forma activa. • CU07: Valorar lo que suponen las nuevas formas de trabajo actuales, como es el teletrabajo y el trabajo en red, y saber trabajar de forma colaborativa en ellas. • CU08: Entender las prácticas y el trabajo colaborativo como una forma de aplicar la teoría y como una manera de indagar sobre la práctica de valores teóricos.
Resultados de aprendizaje de la asignatura	• Busca y localiza información digital relevante para aplicarla a su ámbito de conocimiento. • Aplica herramientas y recursos para buscar información. • Presenta y difunde información a través de medios digitales con una calidad profesional. • Aplica correctamente estrategias de comunicación y de difusión de información en la red. • Domina los conceptos, las funciones y aplicaciones básicas, dispositivos e interrelación entre programas. • Aplica estrategias de comunicación e interacción en entornos virtuales correctamente. • Usa y aplica críticamente y de forma segura las TIC. • Sabe qué es una amenaza informática, qué intenta dañar o por qué se produce. • Diferencia entre los distintos tipos de amenazas informáticas y sabe cómo minimizar sus daños. • Conoce qué tecnologías están destinadas a la seguridad y su gestión. • Conoce el funcionamiento, los avances técnicos y las limitaciones de la seguridad privada.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	Se aportará formación relacionada con las diferentes tecnologías que ofrecen información sobre diferentes tipos de riesgos, de manera que tienen un papel decisivo en la adopción de medidas de carácter preventivo o medidas correctoras de los parámetros. Tales tecnologías están relacionadas generalmente con riesgos tecnológicos y naturales; se trata de sistemas y redes de información y alerta, como sistemas de información hidrológica, redes de alerta a la radiactividad, sistemas de medición de gases contaminantes, etc. Se conocerán diferentes sistemas de simulación de emergencias, como sismos, maremotos, así como simulaciones de movimientos de masas. La asignatura se completará con el uso de diferentes tecnologías de comunicación para la gestión de emergencias.
Contenidos	**Unidad 1: Seguridad de la información 1** • La administración y organización de la ciberseguridad. • Normalización, homologación, evaluación, certificación y acreditación. Marco legal. • El Sistema de Gestión de la Seguridad de la Información. Familia ISO 27XXX. • El Plan integral de seguridad de los sistemas de información. • Análisis y gestión de riesgos. **Unidad 2: Seguridad de la información 2** • El Plan integral de seguridad de los sistemas de información. • Análisis y gestión de riesgos. • TSCM- technical surveillance counter-measures • **Unidad 3: Vulnerabilidades, amenazas y protocolos de seguridad en las TIC** • Introducción a las redes • Situación de la seguridad de los sistemas y productos informáticos. • Vulnerabilidades en sistemas informáticos. • Tipologia de ataques informaticos. • Análisis y clasificación de los ataques informáticos. • Medidas, servicios y mecanismos de seguridad. • Firma digital. Autoridades de certificación. Infraestructuras de clave pública. Terceros de confianza. • Sistemas de autenticación de varios factores y basados en infraestructuras de clave pública. • Protocolos de seguridad. **Unidad 4: Sistemas y redes de comunicación para seguridad y emergencias** • Fundamentos de los sistemas de comunicaciones. • Técnicas y Sistemas de transmisión. • Teoría de la comunicación. • Teoría de la información • Radiocomunicación. Radiación, propagación y procesado de señales en distintos medios físicos. • Redes de Comunicaciones tácticas (concepto de red celular, tetra, tetrapol, GSM, UMTS.) y estratégicas (fijas y móviles terrenas y satelitales). **Unidad 5: Sistemas tecnologicos** • Concepto de Red celular • Avances del GSM al 5G

	• Sistema de gestión de protocolos de Internet.(IP). • Concepto de Intenet Service Provider (ISP) • Redes VPN **Unidad 6: Protección de Infraestructuras Críticas** • Introducción a la protección de las IC • Sistema de protección de IC en España: Ley 8/2011 y RD 704/2011 • Plan de Seguridad del Operador - PSO • Plan de Protección Específico - PPE • Plan de Apoyo Operativo - PAO • Gestión de riesgos en IC

METODOLOGÍA	
Actividades formativas	**Actividades de descubrimiento inducido (Estudio de Caso).** Actividades en las que el alumno podrá llevar a cabo un aprendizaje contextualizado trabajando, en el Aula Virtual y de manera colaborativa, una situación real o simulada que le permitirá realizar un primer acercamiento a los diferentes temas de estudio. **Actividades de interacción y colaboración (Foros-Debates de apoyo al caso y a la lección).** Actividades en las que se discutirá y argumentará acerca de diferentes temas relacionados con las asignaturas de cada materia y que servirán para guiar el proceso de descubrimiento inducido. **Presentaciones de trabajos y ejercicios propuestos.** Incluye la elaboración conjunta en el Aula Virtual y, en su caso, defensa virtual de los trabajos y ejercicios solicitados conforme a los procedimientos de defensa que se establezcan en las guías docentes. **Tutorías.** Permiten la interacción directa entre docente y alumno/a para la resolución de dudas y el asesoramiento individualizado sobre distintos aspectos de las asignaturas. **Actividades de evaluación.** El sistema de evaluación final será común para todas las asignaturas de la materia y se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. **Actividades de trabajo autónomo individual (Estudio de la lección).** Trabajo individual de los materiales utilizados en las asignaturas, aunque apoyado por la resolución de dudas y construcción de conocimiento a través de un foro habilitado para estos fines. Esta actividad será la base para el desarrollo de debates, resolución de problemas, etc. **Lectura crítica, análisis e investigación.** Se trata de actividades en las que el alumno se acerca a los diferentes campos de estudio con una mirada crítica que le permite un acercamiento a la investigación. Se incluyen, a modo de ejemplo, recensiones de libros o crítica de artículos y proyectos de investigación.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.* El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*. El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera: **Sistema de evaluación convocatoria ordinaria** **Opción 1. Evaluación continua** Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua. Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura. Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua. Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5. **Opción 2. Prueba de evaluación de competencias** Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**. La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final. El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las

competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria.

Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior.

En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado.

En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura.

Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	Artés, A., Pérez, F., Cid, J., López, R., Mosquera, C. y Pérez, F (2007). *Comunicaciones Digitales.* Pearson. Normas de la Autoridad nacional para la protección de la información clasificada. (2012). *Oficina Nacional de Seguridad*. Ministerio de la Presidencia.https://www.buenjuicio.com/wpcontent/uploads/2015/07/Normas_de_la_Autoridad_Nacional_para_la_Proteccion_de_la_Informacion_Clasificada.pdf
BibliografÍa complementaria	Fernández, C. M., & Piattini, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO*. AENOR ediciones. Anderson, R. (2008). *Security Engineering: A guide to Building Dependable Distributed Sistems.* Wiley. Pfleeger, C.P., y Pfleeger, S. L. (2007) *Security in Computing*. Prentice Hall. Vacca, John R. (2009). *Computer and Information Security Handbook.* Morgan Kaufmann Publishers Inc. Gómez, L.A. y Fernández, P. (2018) *Como implantar un SGSI según UNE-ISI/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad*. AENOR INTERNACIONAL, S.A.U. Tecnología de la información. Técnicas de seguridad. Sistema de gestión de seguridad de la información. Visión general y vocabulario. ISO/IEC 27000:2014. AENOR INTERNACIONAL, S.A.U. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. (2011). *Boletín Oficial de Estado, 121, sec. I, de 21 de mayo de 2011, 50808 a 50826.* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-8849 Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. (2011). *Boletín Oficial del Estado,102, sec. I, de 29 de mayo de 2011.* https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630
Otros recursos	Dado que este docente, imparte clases en directo que permanecen grabadas en cada unidad y en virtud del desarrollo de estas, se podrá añadir recursos complementarios en la propia unidad didáctica.