Guía Docente: Autenticación y Sistemas Biométricos

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Grado en Ingeniería Informática
Plan de estudios	2012
Especialidad/Mención	Mención en Criptología y Seguridad de la Información
Materia	Criptología y Seguridad de la Información
Carácter	Optativo
Período de impartición	Tercer Trimestre
Curso	Cuarto
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	Ninguno

DATOS DEL PROFESORADO			
Profesor Responsable	Antonio Juan Jiménez Masot	**Correo electrónico**	antoniojuan.jimenez.masot@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	https://es.linkedin.com/in/ajjmasot		

Profesor	Sergio Trilles Oliver	**Correo electrónico**	sergio.trilles@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	**Web personal**		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Auditoría y seguridad avanzada de sistemas y redes de comunicaciones • Autenticación y Sistemas Biométricos • Criptografía y Criptoanálisis • Dirección de Proyectos de Seguridad Corporativos • Técnicas de Análisis Forense • Técnicas de auditoría, ataque y programación segura de aplicaciones web
Contexto y sentido de la asignatura en la titulación y perfil profesional	Con esta asignatura nos introduciremos en el apasionante mundo de la biometría. Para ello, la definiremos y veremos las características que debe cumplir un rasgo o comportamiento humano, para que lo podamos considerar como medible biométricamente hablando. De igual forma, distinguiremos entre la biometría fisiológica, como puede ser el reconocimiento facial, y la biometría que estudia algún comportamiento humano, como por ejemplo la firma manuscrita o la forma de andar. Nos centraremos en las partes que debe tener todo control de acceso, y en qué lugar del mismo, puede ayudarnos la biometría para hacer más seguro y fiable dicho acceso. También veremos la diferencia entre identificación y verificación, así como los diferentes subsistemas que conforman un sistema biométrico. Seguidamente nos iremos centrando en los diferentes sistemas biométricos en particular: reconocimiento de huella dactilar, reconocimiento facial, reconocimiento de la retina y el iris ocular, reconocimiento por la voz, etc. En definitiva, veremos cómo nos puede ayudar la biometría para implementar un control de acceso efectivo, y se presentarán las principales técnicas biométricas. Esta materia se engloba dentro de la Mención de Criptología y Seguridad de la Información.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CMC-07 - Conocimiento y aplicación de los principios fundamentales y técnicas básicas de autenticación de personas físicas y sistemas informáticos, incluyendo los sistemas biométricos y de doble factor. • CU2 - Identificar y dar valor a las oportunidades tanto personales como profesionales, siendo responsables de las actuaciones que se pongan en marcha, sabiendo comprometer los recursos necesarios, con la finalidad de realizar un proyecto viable y sostenible para uno mismo o para una organización. • CU10 - Reconocer y saber resolver problemas que afecten a derechos fundamentales de las personas y a valores democráticos. • CU17 - Ser capaz de concluir adecuadamente la tesis de la exposición basándose en modelos, teorías o normas, etc. • CT-01 - Capacidad de análisis y síntesis: encontrar, analizar, criticar (razonamiento crítico), relacionar, estructurar y sintetizar información proveniente de diversas fuentes, así como integrar ideas y conocimientos. • CT-03 - Capacidad de comunicación oral y escrita en el ámbito académico y profesional, con especial énfasis en la redacción de documentación técnica. • CT-04 - Capacidad para la resolución de problemas. • CT-06 - Capacidad de trabajo en equipo. • CT-09 - Capacidad para innovar y generar nuevas ideas.
Resultados de aprendizaje de la asignatura	• Conoce los sistemas de autenticación biométricos más utilizados, así como sus principales características, nivel de seguridad que proporcionan y ventajas e inconvenientes de cada uno de ellos. • Conocimiento y aplicación de los principios fundamentales y técnicas básicas de autenticación de personas físicas y sistemas informáticos, incluyendo los de doble factor. • Plantea, desarrolla y dirige el proyecto de implantación de un sistema de autenticación, tanto en un entorno físico como telemático, evaluando aspectos técnicos, humanos y económicos. • Conoce y es consciente de los aspectos legales y relacionados con la privacidad de las personas que conllevan algunos sistemas de autenticación.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	Otro de los grandes pilares de la Seguridad de la Información lo constituyen los procesos de autenticación. En esta asignatura se estudian los mismos, con especial hincapié en los sistemas biométricos. Se analizan sus ventajas e inconvenientes, su fiabilidad, a través de las diferentes tasas de falsos positivos y negativos, y, finalmente, los aspectos relacionados con su seguridad.
Contenidos	**UD 1: Introducción a la biometría** • Control de acceso y técnicas de autenticación • Definición y cronología de la biometría • Técnicas de autenticación biométrica • Biometría frente otras técnicas • Características biométricas • Identificación frente a verificación **UD 2: Fundamentos de los sistemas biométricos** • Procedimiento general en un sistema biométrico • Componentes de un sistema biométrico • Proceso de verificación o identificación • Rendimiento y evaluación de los sistemas biométricos • Ventajas y desventajas de la biometría • Gestión de riesgos en biometría **UD 3: Huellas dactilares** • Formación características de las huellas dactilares • Adquisición de las huellas dactilares • Extracción de características • Comparación de huellas • Ataques a sistemas de reconocimiento de huella dactilar **UD 4: Técnicas biométricas. Facial, iris, retina, forma de caminar** • Reconocimiento facial • Reconocimiento por iris • Reconocimiento por retina • Reconocimiento por la forma de caminar **UD 5: Técnicas biométricas. Voz y firma.** • Reconocimiento de locutor • Reconocimiento por firma escrita **UD 6: Técnicas biométricas. Mano. Sistemas multibiométricos** • Sistema de reconocimiento a través de la huella de la mano • Sistemas multibiométricos • Biometría y normativa

METODOLOGÍA	
Actividades formativas	Para el desarrollo de la asignatura se llevarán a cabo las siguientes actividades: • **Estudio de caso:** Se plantearán estudios de caso en varias unidades didácticas sobre algún tema de la unidad. Se trata de estudiar algún tema en el que se deberá investigar en la web para resolverlo y donde el alumno deberá utilizar los recursos necesarios aplicando los conceptos y aspectos desarrollados en las unidades didácticas. • **Foros de Debate:** actividad en la que se discutirá y argumentará acerca de diferentes temas relacionados con la asignatura. • **Trabajo colaborativo:** en esta tarea se deberá reflexionar sobre alguno de los temas planteados y entablar un diálogo y debate con el resto de estudiantes para presentar un trabajo conjunto. • **Cuestionarios:** cuestionario evaluable que servirán para poner a prueba los conocimientos adquiridos. • **Actividades de contenidos:** Al igual que el cuestionario, pone a prueba los conocimientos adquiridos mediante la resolución de ejercicios prácticos. • **Tutorías:** Se realizarán tres tutorías síncronas a lo largo del trimestre donde se expone la resolución de las dudas presentadas al profesor previamente. Una vez realizadas pueden visualizarse en diferido. • **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. **Prueba de Evaluación por Competencias (PEC)**: En el caso de optar por la opción 2 de evaluación (PEC+ examen final), el estudiante tendrá que realizar la prueba de evaluación de competencias (PEC). Esta prueba se define como una actividad integradora a través de la cual el estudiante deberá demostrar la adquisición de competencias propuestas en la asignatura, vinculadas principalmente al «saber hacer». Para ello hará entrega de un conjunto de evidencias en respuesta a los retos propuestos en esta prueba. La entrega se realizará antes de finalizar la asignatura.

EVALUACIÓN	
Sistema evaluativo	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.

Características de los exámenes

Los exámenes constarán de 30 ítems compuestos por un enunciado y cuatro opciones de respuesta, de las cuales solo una será la correcta. Tendrán una duración de 90 minutos y la calificación resultará de otorgar 1 punto a cada respuesta correcta, descontar 0,33 puntos por cada respuesta incorrecta y no puntuar las no contestadas. Después, con el resultado total, se establece una relación de proporcionalidad en una escala de 10.

	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	[1] Observatorio de la Seguridad de la Información. Estudio sobre las tecnologías biométricas aplicadas a la seguridad. Observatorio de la Seguridad de la Información, 2011. [Online]. Available: https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=1667 Obra avalada por expertos del mundo de la biometría que exponen sus experiencias al respecto. Es una buena obra de inicio para adentrarse en el mundo de la biometría, en el que se expone de forma somera los diferentes sistemas biométricos sin adentrarse en el mundo matemático que hay detrás del mismo. Destacar los ejemplos de uso real de los sistemas de reconocimiento biométricos, como por ejemplo para el control aeroportuario. [2] Tapiador Mateos, M. y Sigüenza Pizarro, J. A., *Tecnologías biométricas aplicadas a la seguridad*. Madrid: Ra-Ma. 2005.

	Libro de referencia en el mundo de la biometría. Este libro es de un nivel avanzado, ya que específica con precisión el campo matemático y probabilístico que hay detrás del reconocimiento biométrico. De igual forma, explica de forma precisa y extensa los diferentes métodos de reconocimiento biométrico tanto estáticos (huella dactilar, iris y retina, geometría de la mano), como dinámicos (voz, firma y escritura, dinámica de tecleo). También, incluye aspectos relacionados con la estandarización, así como en el mundo de la biometría forense.
Bibliografía complementaria	[1] N. Aguerre & V. Kannemann. Biometrías 2. Buenos Aires: Jefatura de Gabinetes de Ministros, 2011. [2] Alonso, P. Análisis del algoritmo DTW para reconocimiento biométrico de personas mediante firma manuscrita on-line. Madrid: Universidad Carlos III, 2012. [3] Blázquez, L. *Reconocimiento Facial Basado en Puntos Característicos de la Cara en entornos no controlados*. Madrid: UAM, 2013. [4] Butrón, J. *Autenticación Biométrica por Huella Dactilar en estadios*. Universidad del Aconcagua, 2012. [5] Conde, C. *Verificación facial multimodal: 2D y 3D.* Madrid: Universidad Rey Juan Carlos, 2006. [6] Corredera, P. y Gutiérrez, F. *Una década del Instituto de Física Aplicada. 1995-2005*. 149-155. Madrid: CSIC, 2007. Recuperado el 25 de Julio de 2016, de http://digital.csic.es/bitstream/10261/2744/1/Una%20d%C3%A9cada%20del%20IFA,%201995-2005.pdf [7] Faisal, M., Zaheer, Z. & Khurshid, J. (2013). Novel Iris Segmentation and Recognition System for Human Identication 2013. Recuperado el 20 de Agosto de 2016, de https://www.researchgate.net/publication/261308377_Novel_iris_segmentation_and_recognition_system_for_human_identification [8] Faúndez, M. & Sesa-Nogueras, E. Jornadas sobre Reconocimiento Biométricos de personas. Aplicaciones biométricas más allá de la seguridad, 25-43. Las Palmas de Gran Canaria, 2012. Recuperado el 20 de agosto de 2016 de, http://www.grafologiauniversitaria.com/aplicaciones_biometricas_mas_alla_de_la_seguridad.pdf [9] García, A. *Aceleración con GPU de algoritmos de reconocimiento biométrico mediante firma manuscrita on-line.* Madrid: Universidad Carlos III, 2013. [10] González, M. *Reconocimiento de iris*. Barcelona: UAB, 2012. [11] Karthikeyan, V. & Vijayalakshmi, V. J. AnEfficient Method for Recognizing the Low Quality Fingerprint Verification by Means of Cross Correlation. IJCI, 2013. Recuperado el 29 de Junio de 2016, de https://arxiv.org/ftp/arxiv/papers/1311/1311.3076.pdf [12] Negin, M., Chmielewsk, T. A., Salganicoff, M., Camus, T. A., Cahn von Seelen, U. M., Venetiane, P. L. & Zhang, G. G. An Iris Biometric System for Public and Personal Use. IEEE, 70-75, 2000. Recuperado el 10 de Agosto de 2016, de http://ai.pku.edu.cn/aiwebsite/research.files/collected%20papers%20-%20others/An%20iris%20biometric%20system%20for%20public%20and%20personal%20use.pdf [13] Observatorio de la Seguridad de la Información. *Guía sobre las tecnologías biométricas aplicadas a la seguridad*. Madrid: INTECO, 2011. [14] Sánchez, R. El iris ocular como parámetro para la identificación biométrica. *Agora*

SIC, 2000. Recuperado el 10 de Junio de 2016 de, http://www.revistasic.com/revista41/pdf_41/SIC_41_agora.PDF

[15] Sánchez-Reillo, R. & González-Marcos, A. Access Control System with Hand Geometry Verification and Smart Cards. IEEE, 2000. Recuperado el 17 de Junio de 2016, de http://ai.pku.edu.cn/aiwebsite/research.files/collected%20papers%20-%20fingerprint/Access%20control%20system%20with%20hand%20geometry%20verification%20and%20smart%20cards.pdf

[16] UMANICK. *Introducción a la Biometría: La biometría como única forma segura de identificación inequívoca de las personas*. Valencia: UMANICK, 2014.

[17] Zhao, W., Chellappa, R., Phillips, P. J. & Rosenfeld, A. Face Recognition: A Literature Survey. *ACM Computing Surveys*, 399–458, 2003. Recuperado el 22 de Julio de 2016, de http://nichol.as/papers/ZHAO/Face%20Recognition:%20A%20Literature%20Survey.pdf

Otros recursos

[1] BBC. Escándalo en Brasil por dedos de "empleados fantasma", 2013. Recuperado el 27 de Febrero de 2019, de http://www.bbc.com/mundo/noticias/2013/03/130312_curiosidades_brasil_dedos_silicona_rg

[2] ElEconomista.es. Barclays usará biométrica de venas para luchar contra el fraude bancario, 2014. Recuperado el 27 de Febrero de 2019, de http://www.eleconomista.es/empresas-finanzas/noticias/6059786/09/14/Barclays-usara-biometrica-de-venas-para-luchar-contra-el-fraude-bancario.htm

[3] Kimaldi. Pago a través de un sistema biométrico de huella digita, 2015. Recuperado el 27 de Febrero de 2019, de http://www.kimaldi.com/sectores/hoteles_y_restauracion/pago_a_traves_de_un_sistema_biometrico_de_huella_digital

[4] López, N. Técnicas de biometría basadas en patrones faciales del ser humano. Universidad Tecnológica de Pereira, 2012. Recuperado el 5 de Julio de 2016 de, http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2738/0053682L864.pdf;jsessionid=95FB5EB63B0FB3C4514C650E583574D8?sequence=1

[5] Maya, A. Sistema biométrico de reconocimiento de huella dactilar en control de acceso de entrada y salida. Bogotá: Universidad Militar Nueva Granada, 2013. Recuperado el 1 de Agosto de, http://repository.unimilitar.edu.co/bitstream/10654/11168/1/MayaVargasAdriana2013.pdf

[6] National Institute of Standards and Technology. Estudios y proyectos sobre biometría, 2016. Recuperado el 27 de Febrero de 2019, de http://www.nist.gov/biometrics-portal.cfm

[7] Samper, E. Personas que no dejan huella, 2008. Recuperado el 11 de Agosto de 2016, de http://www.soitu.es/soitu/2008/04/01/salud/1207067071_846773.html

[8] Sanz, S. Desarrollo y comparación de sistemas de reconocimiento biométrico de personas usando características de la forma de andar. Madrid: UAM, 2012. Recuperado el 8 de Agosto de 2016 de, http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20121218SilviaGabrielSanz.pdf

[9] Serratosa, F. La biometría para la identificación de las personas. Barcelona: UOC, 2010. Recuperado el 7 de Julio de 2016 de, https://www.exabyteinformatica.com/uoc/Biometria/Biometria_ES/Biometria_ES_(Modulo_1).pdf

[10] Welivesecurity. Demuestran que es posible vulnerar lectores de huella digital mediante huellas maestras, 2018. Recuperado el 27 de Febrero de 2019 de https://www.welivesecurity.com/la-es/2018/11/16/demuestran-que-es-posible-vulnerar-lectores-de-huella-digital-mediante-huellas-maestras/