Guía Docente: Biometría Aplicada

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Máster en Ciberseguridad
Plan de estudios	2018
Materia	Tendencias tecnológicas y Ciberseguridad
Carácter	Obligatorio
Período de impartición	Primer Trimestre
Curso	Primero
Nivel/Ciclo	Máster
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No se prevén requisitos previos, por tanto los requisitos serán los propios del título.

DATOS DEL PROFESORADO			
Profesor Responsable	Aurora Sáez Manzano	**Correo electrónico**	aurora.saez@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	Linkedin **Google académico**		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Biometría Aplicada
Contexto y sentido de la asignatura en la titulación y perfil profesional	La biometría se puede definir como el estudio para el reconocimiento inequívoco de personas basado en uno o más rasgos conductuales o físicos intrínsecos. Partiendo de esta definición se introduce esta asignatura. Esta asignatura está ubicada en el máster de Ciberseguridad, dentro del conjunto de materias de “Tendencias tecnológicas y Ciberseguridad” junto con las siguientes asignaturas: Ciberseguridad móvil, Ciberseguridad en Servicios y Aplicaciones web y Ciberseguridad social e industrial. En este sentido, además de adentrarnos en la biometría, estudiando sus características, sistemas y tipos, analizando en detalle sistemas biométricos específicos como huellas dactilares, reconocimiento facial, iris, retina y voz, entre otros, se hará especial mención a los diferentes ataques que pueden sufrir los sistemas de autenticación biométrica así como las buenas prácticas y contramedidas que se pueden llevar a cabo con el objetivo de reducir los riesgos asociados al empleo de la biometría.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	CB6: Poseer y comprender conocimientos que aporten una base u oportunidad de seroriginales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. CB7: Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad deresolución de problemas en entornos nuevos o poco conocidos dentro de contextos másamplios (o multidisciplinares) relacionados con su área de estudio. CB9: Ser capaz de transmitir sus conclusiones, y los conocimientos y fundamentos que lassustentan, a públicos especializados y no especializados de un modo claro y sinambigüedades. CG1: Ser capaz de analizar, sintetizar y organizar la información dentro del área de seguridadinformática y de las comunicaciones CG3: Diseñar y elaborar concisa, clara y razonadamente planes y proyectos de trabajo en elámbito de la ciberseguridad. CG5: Ser capaz de proponer soluciones imaginativas y originales así como ser capaz depromover la innovación e identificación de alternativas contrapuestas a los métodos yenfoques tradicionales en el ámbito de la ciberseguridad CE08: Conocer, aplicar y evaluar técnicas avanzadas de autenticación biométrica de accesoa sistemas. CE11: Conocer, aplicar y evaluar métodos y técnicas para la seguridad de sistemastecnológicos sociales (IoT) e industriales (IIoT).
Resultados de aprendizaje de la asignatura	• Adquirir las competencias básicas y generales detalladas anteriormente. • Adquirir los conceptos sobre las técnicas de autenticación biométricas más utilizadas • Adquirir conceptos necearios para desarrollar y evaluar un sistema de autenticación biométrica. • Conocer la normativa aplicable a los sistemas de autenticación.

PROGRAMACION DE CONTENIDOS	

Breve descripción de la asignatura	En esta asignatura se verá, entre otros:
	
	• Técnicas de autenticación:
	  ◦ Control de acceso.
	  ◦ Técnicas de autenticación.
	  ◦ Técnicas biométricas de autenticación.
	  ◦ Ventajas e inconvenientes.
	• Fundamentos biométricos:
	  ◦ Gestión de riesgos en biometría.
	  ◦ Buenas prácticas de autenticación de sistemas biométricos
	  ◦ Normativa aplicable.
	• La huella dactilar.
	  ◦ Adquisición de huellas y reconocimiento.
	  ◦ Comparación y extracción de datos
	  ◦ Ataques a sistemas de autenticación biométrica de huella dactilar

	• Reconocimiento facial.
	  ◦ Reconocimiento por iris y retina.
	  ◦ Comparación y extracción de datos
	  ◦ Ataques a sistemas de autenticación biométrica de reconocimiento facial
	• Reconocimiento de voz:
	  ◦ Adquisición de sonido.
	  ◦ Comparación y extracción de datos
	  ◦ Ataques a sistemas de autenticación biométrica de reconocimiento de voz
	• Otras técnicas biométricas:
	  ◦ Reconocimiento de la mano
	  ◦ Reconocimiento de la firma escrita.
	  ◦ Combinación de técnicas biométricas

Contenidos	**Unidad Didáctica 1. Técnicas de autenticación** • Control de acceso • Técnicas de autenticación • Técnicas biométricas de autenticación • Características biométricas • Ventajas e inconvenientes **Unidad Didáctica 2. Fundamentos biométricos** • Funcionamiento y rendimiento de un Sistema Biométrico • Seguridad en los sistemas biométricos • Buenas prácticas de autenticación de sistemas biométricos • Normativa aplicable **Unidad Didáctica 3. Huellas dactilares** • Crestas de fricción • Adquisición de huellas dactilares • Extracción de características y comparación • Ataques **Unidad Didáctica 4. Reconocimiento de iris y retina** • Sistema de reconocimiento de iris • Ataques a un sistema biométrico por iris • Sistema de reconocimiento de retina **Unidad Didáctica 5. Reconocimiento facial y de voz** • Sistema de reconocimiento facial • Sistema de reconocimiento de locutor **Unidad Didáctica 6. Geometría de la Mano. Firma. Sistemas multibiométricos.** • Reconocimiento de la geometría de la mano • Reconocimiento de firma • Sistemas multibiométricos

METODOLOGÍA	
Actividades formativas	Para el desarrollo de la asignatura se llevarán a cabo las siguientes actividades: **Foros de debate:** actividad en la que se discutirá y argumentará acerca de diferentes temas relacionados con la asignatura **Estudios de caso:** actividad en la que el alumno podrá llevar a cabo un aprendizaje contextualizado trabajando una situación real o simulada que le servirá para guiar el proceso de descubrimiento inducido. **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.

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	Jain, A., Ross, A., and Nandakumar, K. (2011) *Introduction to Biometrics.* Springer Science & Business Media Libro de texto sobre biometría, que proporciona una introducción a los conceptos y metodologías básicas para el reconocimiento biométrico. Se centra en las técnicas clave que se utilizan ampliamente en la comunidad de biometría, y en los tres rasgos más utilizados: la huella dactilar, la cara y el iris, aunque también se analizan otros rasgos biométricos, así como de la seguridad. Reid P. *Biometrics and Network Security* (2003) Prentice Hall PTR Upper Saddle River, NJ, USA Libro que realiza un recorrido por las diferentes técnicas de reconocimiento biométrico centrándose en el aspecto de la seguridad.
Bibliografía complementaria	Akran, N. And Khan, S. (2011) Retinal recognition: Personal identification using blood vessels. *6th International Conference on Internet Technology and Secured Transactions*, Abu Dhabi, United Arab Emirates Bhattacharyya, D., Ranjan, R., Alisherov, F., and Choi, M. (2009) Biometric Authentication: A Review. *International Journal of u- and e- Service, Science and Technology, 2* (3). Daugman, J.G. (2004) How Iris Recognition Works. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 21-30. Maltoni D., and Raffaele C. (2008) *Fingerprint Recognition*. *Handbook of Biometrics.* Springer Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S. (2002). Impact of artificial gummy fingers on fingerprint systems. In: *Proc. SPIE, Optical Security and Coun-terfeit Deterrence Techniques IV*. 4677, 275–289. Memon, S., Sepasian, M., Balachandran, W. (2009) Review of finger print sensing technologies. *IEEE International Multitopic Conference*, 2008. INMIC 2008. Newman, R. (2009). *Security and Access Control Using Biometric Technologies: Application, Technology, and Management* . Course Technology Press, Boston, MA, United States.

Ross, A., Jain, A. (2007) Human Recognition Using Biometrics: An Overview. *Annals of telecommunication, 62* (1/2), 11-35.

Yang, J., Zhen L., Dong Y., and Stan Z. Li. (2015) Person-specific face antispoofing with subject domain adaptation. *IEEE Transactions on Information Forensics and Security, 10*(4), 797-809.

Van der Putte, T., Keuning, J. (2000). Biometrical fingerprint recognition don't get your fingers burned. *In: IFIP*, 289–303

Otros recursos

European Commission Information System Security Policy (2006) *Standard on access control and authentication.* Recuperado de: https://www.eba.europa.eu/documents/10180/1449046/Annex+7+Standard+on+Access+Control+and+Authentication.pdf/cba4e74d-f54d-4797-9204-6dae43560e65

Emandi, E., Arama, C. (2017) *Biometric systems security*. Recuperado de https://www.anmb.ro/buletinstiintific/buletine/2017_Issue1/FCS/406-412.pdf

Fingerprints™, (2017) *Biometric Technologies*. Recuperado de https://www.fingerprints.com/asset/assets/downloads/fingerprints-biometric-technologies-whitepaper-2017-revb.pdf

Freije, B. (2017). *Datos biométricos tras el nuevo Reglamento General de Protección de Datos*. Recuperado de https://abogadium.com/eltintero/articulo/datos-biometricos-tras-el-nuevo-reglamento-general-de-proteccion-de-datos

Galbally, J. (2009). *Vulnerabilities and attack protection in security systems based on biometric recognition, (Doctoral of Philosphy's thesis, Universidad Autonoma de Madrid)*. Recuperado de: https://pdfs.semanticscholar.org/a323/9de6f4c300b135d5c417890ab68be8e90801.pdf

Haar-like feature. (Sin fecha). En Wikipedia. Recuperado el 24 de Julio de 2018 de https://en.wikipedia.org/wiki/Haar-like_feature

Media (2017) GDPR: Los datos biométricos en el nuevo Reglamento de Protección de Datos. [Mensaje en un blog] Signaturit. Recuperado de https://blog.signaturit.com/es/el-impacto-del-nuevo-reglamento-de-proteccion-de-datos-en-el-tratamiento-de-datos-biometricos

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Recuperado de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Sánchez, M. (2017) Usuarios privilegiados: Cómo controlar su acceso al sistema. [Blog post] Recuperado de: https://ssa-asesores.es/html/wordpress/blog/2017/01/03/controlando-el-acceso-de-los-usuarios-privilegiados/

Schneider, B (2009) Authentication for People. Recuperado de: https://www.cs.cornell.edu/fbs/publications/chptr.AuthPeople.pdf