

## Guía Docente: Biometría Aplicada

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

DATOS DEL PROFESORADO			
<b>Profesor Responsable</b>	Sergio Trilles Oliver	<b>Correo electrónico</b>	sergio.trilles@ui1.es
<b>Área</b>		<b>Facultad</b>	Facultad de Ciencias y Tecnología
<b>Perfil Profesional 2.0</b>	<a href="#">Web personal</a>		

## CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA

<b>Asignaturas de la materia</b>	<ul style="list-style-type: none"> <li>• Biometría Aplicada</li> <li>• Ciberseguridad en Servicios y Aplicaciones Web</li> <li>• Ciberseguridad Móvil</li> <li>• Ciberseguridad Social e Industrial</li> </ul>
<b>Contexto y sentido de la asignatura en la titulación y perfil profesional</b>	<p>La biometría se puede definir como el estudio de las técnicas de reconocimiento inequívoco de personas basado en uno o más rasgos conductuales o físicos intrínsecos. Partiendo de esta definición se introduce esta asignatura.</p> <p>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.</p> <p>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.</p>

## COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE

<b>Competencias de la asignatura</b>	<ul style="list-style-type: none"> <li>• CB6: Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.</li> <li>• CB7: Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.</li> <li>• CB9: Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.</li> <li>• CG1: Ser capaz de analizar, sintetizar y organizar la información dentro del área de seguridad informática y de las comunicaciones.</li> <li>• CG3: Diseñar y elaborar concisa, clara y razonadamente planes y proyectos de trabajo en el ámbito de la ciberseguridad.</li> <li>• CG5: Ser capaz de proponer soluciones imaginativas y originales así como ser capaz de promover la innovación e identificación de alternativas contrapuestas a los métodos y enfoques tradicionales en el ámbito de la ciberseguridad.</li> <li>• CE08: Conocer, aplicar y evaluar técnicas avanzadas de autenticación biométrica de acceso a sistemas.</li> <li>• CE11: Conocer, aplicar y evaluar métodos y técnicas para la seguridad de sistemas tecnológicos sociales (IoT) e industriales (IIoT).</li> </ul>
<b>Resultados de aprendizaje de la asignatura</b>	<ul style="list-style-type: none"> <li>• Adquirir las competencias básicas y generales detalladas anteriormente.</li> <li>• Adquirir los conceptos sobre las técnicas de autenticación biométricas más utilizadas</li> <li>• Adquirir conceptos necesarios para desarrollar y evaluar un sistema de autenticación biométrica.</li> <li>• Conocer la normativa aplicable a los sistemas de autenticación.</li> </ul>

**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 de un sistema biométrico
- Rendimiento de un sistema biométrico
- Seguridad en los sistemas biométricos. Tipos de ataques
- Ataques internos
- Ataques de infraestructura
- Buenas prácticas de autenticación de sistemas biométricos
- Normativa aplicable

**Unidad Didáctica 3. Huellas dactilares**

- Crestas de fricción
- Adquisición de huellas dactilares
- Extracción de características
- Comparación
- Ataques

**Unidad Didáctica 4. Reconocimiento ocular**

- Sistema de reconocimiento de iris
- Ataques a un sistema biométrico por iris
- Sistema de reconocimiento de retina
- Iris frente a retina

#### Unidad Didáctica 5. Reconocimiento facial y de locutor

- Sistema de reconocimiento facial
- Sistema de reconocimiento de locutor

#### Unidad Didáctica 6. Mano. Firma. Sistemas multibiométricos.

- Reconocimiento de la mano
- Reconocimiento de firma
- Sistemas multibiométricos

## METODOLOGÍA

### Actividades formativas

Para el desarrollo de la asignatura si se elige la opción Evaluación continua + examen 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.

En el caso de optar por la opción de evaluación (PEC+ examen final), el estudiante tendrá que realizar la prueba de evaluación de competencias (PEC).

#### Prueba de Evaluación por 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.

\* Los estudiantes que realicen el máster por formación bonificada (FUNDAE) deberán acogerse a la opción 1 del sistema de evaluación, evaluación continua (EC)+ examen final (EX).

### **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

<p><b>Bibliografía básica</b></p>	<p>[1] A. K. Jain and A. A. Ross and N. Karthik, «Introduction to Biometrics». Springer, 2011. Disponible en: <a href="https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=1837">https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=1837</a></p> <p>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.</p> <p>[2] R. Das, «The science of biometrics». Routledge, 2018. Disponible en: <a href="https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=2233">https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=2233</a></p>
<p><b>Bibliografía complementaria</b></p>	<p>[1] M. S. Obaidat, «Biometric-based physical and cybersecurity systems». Springer, 2019. Disponible en: <a href="https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=2234">https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=2234</a></p> <p>[2] Inteco, «Estudio sobre las tecnologías biométricas aplicadas a la seguridad». Observatorio de la Seguridad de la Información, 2011. [Online]. Disponible en: <a href="https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=1667">https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=1667</a></p> <p>[3] K. Ankit y J. Rekha, «Biometrics as a Cryptographic Method for Network Security», <i>Indian J. Sci. Technol.</i>, vol. 9, n.o 22, pp. 1-6, jun. 2016.</p> <p>[4] M. U. Akram, A. Tariq, y S. A. Khan, « Retinal recognition: Personal identification using blood vessels», en <i>6th International Conference on Internet Technology and Secured Transactions</i>, 2011.</p>
<p><b>Otros recursos</b></p>	<p>[1] Recfaces, «The History of Biometrics: From the 17th Century to Nowadays», <i>Recfaces</i>, 2020. [En línea]. Disponible en: <a href="https://recfaces.com/articles/history-of-biometrics">https://recfaces.com/articles/history-of-biometrics</a>. [Accedido: 21-jun-2023].</p> <p>[2] M. Clark, «Biometric Authentication Now and Then: History and Timeline», <i>Bayometric</i>, 2018. [En línea]. Disponible en: <a href="https://www.bayometric.com/biometric-authentication-history-timeline/">https://www.bayometric.com/biometric-authentication-history-timeline/</a>. [Accedido: 21-jun-2023].</p> <p>[4] Information Technology Services, «IT Access, Authorization and Authentication Standard», <i>Florida State University</i>, 2020. [En línea]. Disponible en: <a href="https://its.fsu.edu/cybersecurity/standards/it-access-authorization-and-authentication-standard">https://its.fsu.edu/cybersecurity/standards/it-access-authorization-and-authentication-standard</a>. [Accedido: 21-jun-2023].</p> <p>[5] I. Souka, «Standard on Access Control and Authentication», <i>Eur. Comm. Inf. Syst. Secur. Policy</i>, n.o 352, 2011. [En línea]. Disponible en: <a href="https://www.eba.europa.eu/documents/10180/1449046/Annex+7+Standard+on+Access+Control+and+Authentication.pdf/cba4e74d-f54d-4797-9204-6dae43560e65">https://www.eba.europa.eu/documents/10180/1449046/Annex+7+Standard+on+Access+Control+and+Authentication.pdf/cba4e74d-f54d-4797-9204-6dae43560e65</a></p> <p>[6] E. E. Emandii y C. Aram?, «BIOMETRIC SYSTEMS SECURITY», <i>Sci. Bull. Nav. Acad.</i>, 2017. Disponible en: <a href="https://www.anmb.ro/buletinstiintific/buletine/2017_Issue1/FCS/406-412.pdf">https://www.anmb.ro/buletinstiintific/buletine/2017_Issue1/FCS/406-412.pdf</a></p> <p>[7] N. Nguyen y E. Kaufman, «Biometric Technologies», en <i>Whitepaper</i>, 2017. Fingerprints™, Disponible en: <a href="https://www.fingerprints.com/asset/assets/downloads/fingerprints-biometric-technologies-whitepaper-2017-revb.pdf">https://www.fingerprints.com/asset/assets/downloads/fingerprints-biometric-technologies-whitepaper-2017-revb.pdf</a></p>