## 

**ACTIVIDAD 1.13 SISTEMAS BIOMÉTRICOS**



Daniel Escaño Hernández 2º ASIR

**Índice:**

[**1. Práctica en cuestión**](#_96f644e57iqd) **2**

## **1. Práctica en cuestión**

Averigua si se puede hackear un sistema de reconocimiento facial.

**Un modelo de reconocimiento facial se puede hackear.** Esta es la conclusión de una investigación elaborada por técnicos de McAfee

Los sistemas de reconocimiento facial más habituales son los que utilizan la inteligencia artificial (IA) o el aprendizaje automático para detectar patrones en las caras de los usuarios.

A priori podría decirse que una cámara registra patrones en los rostros de los individuos y los compara con fotos almacenadas en una base de datos: tamaño de los ojos, distancia entre las cejas, ángulo de la nariz... Cualquier detalle es esencial para el sistema.

Basta imaginarse dos sistemas de inteligencia artificial enfrentados, jugando entre sí.

El propósito: confundir al sistema de reconocimiento facial elegido para que confunda el rostro de uno con el de otro.

Proveyeron a las redes neuronales artificiales **un set con 15.000 imágenes suyas.**

Y poco a poco así fueron confundiendo poco a poco al sistema de aprendizaje automático.

Por supuesto, este tipo de hackeo no sería funcional hoy por hoy en un entorno real.

Se deberían reunir demasiados condicionantes para que unos atacantespudiesen explotar en muy poco tiempo a una arquitectura de reconocimiento facial.

Sin embargo, es posible.

