Apelidos, nome /Apellidos, nombre:	DNI:	e-mail:	Teléfono de contacto:
SILVELO PALLÍN, ARTURO			
Título: GRADO EN INGENIERÍA INFORMÁTICA			**Mención cursada:** TECNOLOGÍA DE LA INFORMACIÓN

Resumo / Resumen:

Desde los inicios de la informática los modelos de autenticación han sido un componente esencial para la seguridad de la información. Con el paso del tiempo estos mecanismos se han adaptado a los nuevos dispositivos y tecnologías que han aparecido, y es que hoy en día los teléfonos móviles representan una herramienta indispensable para realizar cualquier operación cotidiana. Sin embargo, los mecanismos de autenticación empleados habitualmente presentan ciertas deficiencias que provocan vulnerabilidades en el sistema: contraseñas poco seguras, pérdida de contraseñas, etc. Por estas razones, se han implementado nuevos sistemas de autenticación más seguros como los sistemas biométricos, los cuales emplean rasgos únicos del ser humano como contraseñas. Aun así, estos sistemas de autenticación siguen presentando un problema común, solo verifican la legitimad del usuario al inicio de la sesión y no durante la misma.

En este trabajo se planteó un modelo de autenticación continuo basado en el comportamiento del usuario frente al uso del dispositivo móvil. Este modelo se presenta como un segundo factor de autenticación, el cuál verifica la legitimidad del usuario de manera transparente para este, pudiendo de esta manera detectar si el usuario que está trabajando en la sesión es el que originalmente se autenticó. Para este propósito fue necesario desarrollar una aplicación multiplataforma que recopilase la información necesaria para generar los perfiles de cada usuario, utilizando para ello los sensores de movimientos disponibles en el dispositivo (acelerómetro y giroscopio) así como los eventos calculados a partir de la pantalla táctil. Los eventos obtenidos mediante los sensores de movimiento fueron agrupados en ventanas de tiempo y, los eventos obtenidos por la pantalla táctil se agruparon en gestos (*swipe, rotate, tap, press, princh, pan*) con el fin de obtener mejores patrones que permitan la identificación de los usuarios.

Para el proceso de análisis de esta información se emplearon diferentes técnicas de Inteligencia Artificial, con el fin de obtener un conjunto de algoritmos que permitiesen la generación de perfiles individuales para la identificación del usuario. Para la creación de estos perfiles se emplearon diferentes técnicas de clasificación, obteniendo durante el proceso múltiples combinaciones de eventos y algoritmos. Los perfiles creados para cada uno de estos usuarios fueron integrados en un servidor para implementar un servicio en línea que permite la identificación de un usuario en tiempo real.

Este trabajo ha sido presentado en el Workshop Machine Learning Galicia 2019 y ha sido premiado con un Accésit por la Cátedra de R en Ciberseguridad.

Posibles aplicacións / Posibles aplicaciones:

Este modelo permitiría evitar ciertos fraudes. En concreto actualmente estamos trabajando con empresas del sector TIC para mejorar la supervisión de situaciones concretas, como son:

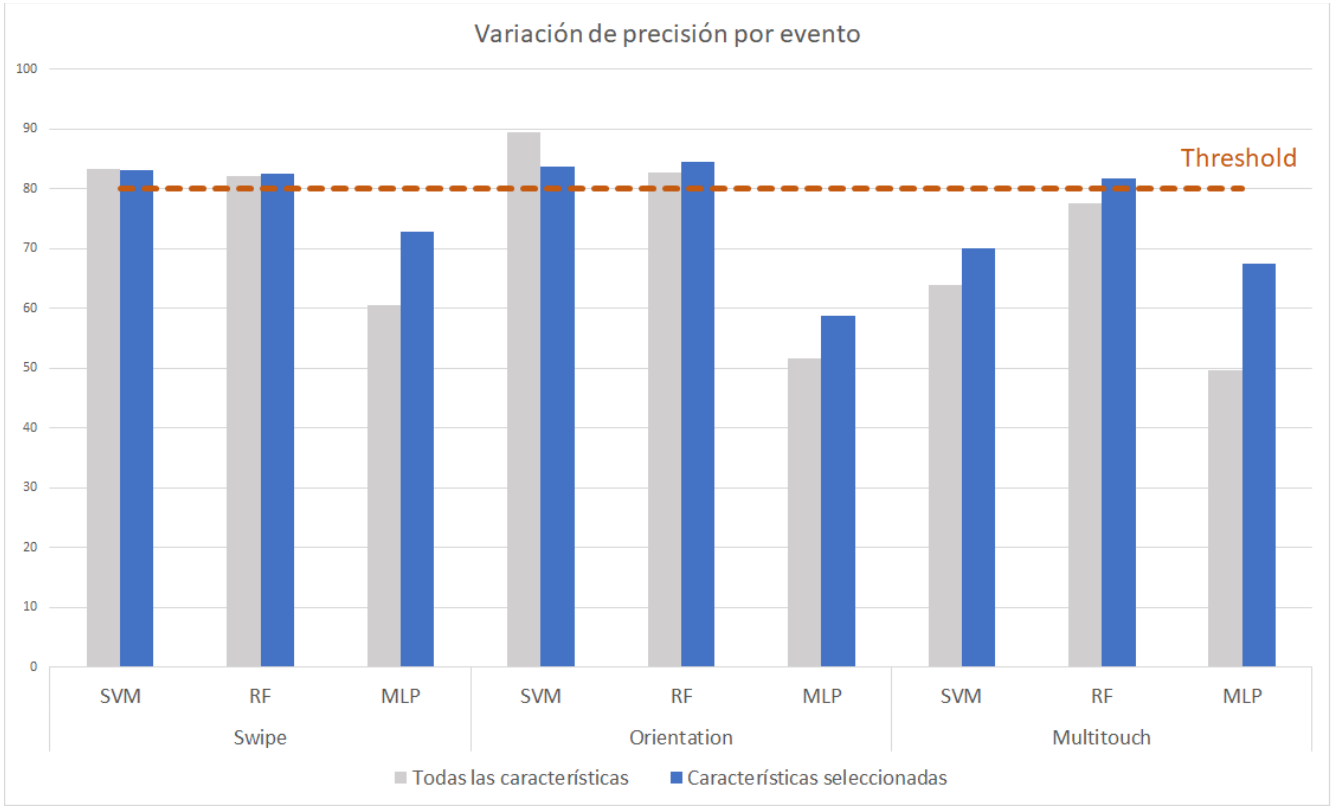
- En el ámbito bancario, actualmente en desarrollo, permite comprobar si se realizan operaciones no autorizadas, como por ejemplo una transferencia. Al llevar a cabo dicha operación el sistema comprobaría en todo momento que el usuario que realiza la transición es legítimo y en caso negativo evitaría que se llevara a cabo.
- Accesos a servicios accesibles desde el exterior, podría controlar que los usuarios que tienen un acceso legítimo no cedan sus sesiones a otros empleados, esto aseguraría que el usuario que utiliza el servicio sea el que dice ser y no permitiría la compartición de sesiones.
- En hospitales, donde el equipo sanitario emplea sistemas informáticos para gestionar los historiales de los pacientes y evolución del tratamiento de les está siendo aplicado. Es conocido que durante la jornada laboral el primero que inicia una sesión no suele cerrarla al finalizar la tarea, generalmente por comodidad y evitar autenticarse continuamente, haciendo que cualquier otro miembro del personal pueda acceder al sistema usando la sesión abierta.

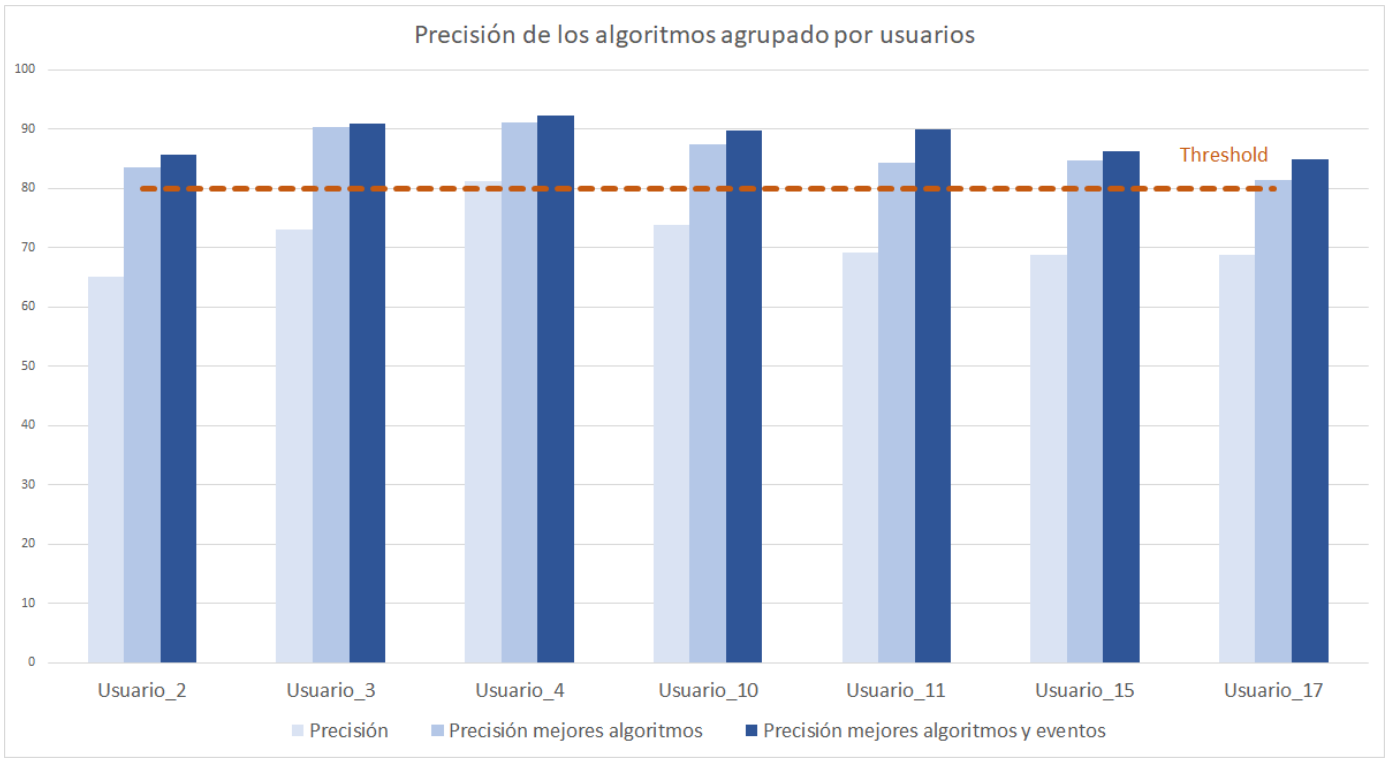
Etapas para o seu desenvolvemento futuro / Etapas para su desarrollo futuro:

A corto plazo está prevista la presentación de una versión de demostración ante una empresa del sector bancario para su implementación. Como parte de este proyecto se está comprobando la viabilidad para extender su uso a entornos de escritorio.

Con la continuación de este proyecto se pretende, ampliar y verificar las técnicas empleadas y llevar a cabo un registro de software que esperamos poder comercializar.

Imaxes representativas / Imágenes representativas:





X	**Autorizo a consulta por parte dos membros da comisión evaluadora da memoria do meu proxecto / Autorizo la consulta por parte de los miembros del tribunal de la memoria de mi proyecto.**

Instruccións para o depósito da memoria / Instrucciones para el depósito de la memoria:

Débese depositar no OneDrive da UDC, dentro da carpeta co seu nome de usuario incluida en:

4 edición - Premio TFG Aplicado (https://udcgal-my.sharepoint.com/:f:/r/personal/nieves_pedreira_udc_es/Documents/4%20edici%C3%B3n%20-%20Premio%20TFG%20Aplicado?csf=1&e=y6SVha)

Se debe depositar en el OneDrive de la UDC, dentro de la carpeta con su nombre de usuario incluida en:

4 edición - Premio TFG Aplicado (https://udcgal-my.sharepoint.com/:f:/r/personal/nieves_pedreira_udc_es/Documents/4%20edici%C3%B3n%20-%20Premio%20TFG%20Aplicado?csf=1&e=y6SVha)