RESUMEN

En los últimos años la implementación del Internet of Things se ha ido incrementando considerablemente, logrando evidenciar ecosistemas IoT en diferentes ámbitos como hogares, compañías, salud, educación, entre otros. Al ser una tecnología reciente las limitaciones de procesamiento, memoria, potencia y la falta de prioridad en la seguridad de algunos dispositivos IoT por parte de los fabricantes, ha dado lugar a una brecha en la seguridad de estos, lo que ha ocasionado problemas a los usuarios y compañías que han decidido utilizar esta tecnología. Una de las principales ventanas para el robo de la información se da en el proceso de autenticación del usuario en las diferentes aplicaciones, ya que este proporciona sus credenciales en internet sin generarse una seguridad adecuada, lo que los vuelve sujetos vulnerables dentro de esta gigantesca red. La propuesta de una metodología de investigación Ad hoc, que como fase inicial contempla tareas de revisiones de literatura, ha permitido identificar y analizar estudios relacionados con la autenticación de ecosistemas IoT, dando apertura a la implementación de un framework de seguridad basado en el protocolo OAuth 2.0. El desarrollo del framework mitigará las vulnerabilidades causadas por ataques como: ataque de fuerza bruta, ataque de suplantación o ataque de hombre en el medio, garantizando de esta manera la seguridad en la autenticación en un ecosistema IoT.

PALABRAS CLAVE:

- **INTERNET OF THINGS**
- **AUTENTICACIÓN**
- **OAUTH 2.0**

ABSTRACT

In recent years, the implementation of the Internet of Things has been increasing, making it possible to demonstrate IoT systems in different areas such as homes, companies, health, education, and others. As a recent technology, the limitations of processing, memory, power and the lack of priority in the safety of some IoT devices by manufacturers has led to a breach in the safety of these devices, which has caused problems for users and companies that have decided to use this technology. One of the main windows for information theft occurs in the process of user authentication in different applications, as this provides their credentials on the Internet without generating adequate security, which makes them vulnerable subjects within this gigantic network. The proposal of an Ad hoc research methodology, that as the initial phase contemplating the literature review tasks, has allowed to identify and analyze the studies related to the authentication of the IoT ecosystems, giving rise to the implementation of a security framework based on the OAuth 2.0 protocol. The development of the framework will mitigate vulnerabilities caused by attacks such as brute force attack, impersonation attack or man attack in the middle, thus guaranteeing authentication security in an IoT ecosystem.

KEY WORDS:

- **INTERNET OF THINGS**
- **AUTHENTICATION**
- **OAUTH 2.0**