Resumen

Uno de los ataques más efectivos en la ciberseguridad, es el de Ingeniería Social, en que el atacante engaña a un usuario final, con la finalidad de perjudicarlo. Existen medidas de hardware y software para hacer frente a este tipo de ataques, sin embargo, las personas en sí son el eslabón más vulnerable en esta cadena de la seguridad, además, se hace la suposición de que características propias del comportamiento de las personas, las hacen más vulnerables, es así que el objetivo de este estudio es determinar cuáles son las características más comunes que hacen vulnerables a estas personas, y qué grupos de personas son más vulnerables. Para esto, se realizó una encuesta a 153 personas, entre docentes, administrativos y estudiantes de una entidad educativa superior, sobre cuatro escalas que toman en cuenta los siguientes comportamientos: comportamiento de riesgo, comportamiento conservador, exposición a la ofensa y percepción al riesgo. Luego, los resultados obtenidos son analizados, obteniéndose que los usuarios que tienen mayor percepción de riesgo, son los que están menos expuestos a un ataque de Ingeniería Social. También se concluye que, los grupos analizados de docentes y administrativos, son menos propensos a ser víctimas de estos ataques, en comparación con los estudiantes, y que las personas que pasan más tiempo frente a un computador, y las que son más permisivas a comportamientos de riesgos, son más vulnerables a estos ataques.

- Palabras claves:
    - **INGENIERÍA SOCIAL**
    - **CIBERSEGURIDAD**
    - **RIESGO**
    - **VULNERABILIDADES**
    - **COMPORTAMIENTO**

Abstract

One of the most effective attacks on cybersecurity is Social Engineering, in which the attacker deceives an end-user to harm him. There are hardware and software countermeasures to deal with these types of attacks. However, people themselves are the most vulnerable link in this security chain. In addition, there are influencing factors in people's behavior, which make them more vulnerable. This study aims to determine the most common characteristics that make users vulnerable, either individually or in groups. For this, we conduct an exploratory and descriptive study on 153 persons among administrative, academics, and students of a superior educational entity on four scales that consider the following behaviors: risk behavior, conservative behavior, exposure to offense, and perception of risk. The results obtained show that the users with the highest risk are the least exposed to a Social Engineering attack. It is also concluded that the analyzed groups of academics and administrators are less likely to be victims of these attacks than students. Finally, it is inferred that people who spend more time in front of a computer and are more permissive of risky behaviors are more vulnerable to these attacks.

- Keywords:
    - **SOCIAL ENGINEERING**
    - **CYBERSECURITY**
    - **RISK**
    - **VULNERABILITIES**
    - **USER BEHAVIOR**