Resumen

La información digital en la actualidad es uno de los recursos más importantes de las personas y empresas, el cibercrimen se presenta como una problemática ya que se dedica a la sustracción de este recurso y ha ido incrementando a través de los años, por ende es primordial implementar en los sistemas informáticos estrategias que mitiguen el robo de datos, frente a esta realidad el presente estudio tiene como objetivo proponer un sistema de autenticación híbrido, agrupando las ventajas de las contraseñas gráficas y las contraseñas de un solo, planteando un mecanismo de autenticación alternativo basado en contraseñas gráficas descartables, sustentado mediante un algoritmo que genera secuencias randómicas, validado por el test de rachas que verifica la aleatoriedad de dichas secuencias y evaluado contra los ataques de robo de credenciales tales como Keylogger, ataque de fuerza bruta o de diccionario y Shoulder Surfing las cuales se presentan como técnicas sencillas de comprender y aplicar para el robo de credenciales, conjuntamente se realizó un proceso de evaluación de usabilidad donde se refleja un 92% de aceptación del mecanismo propuesto, el esquema se desarrolló tomando en cuenta las buenas prácticas y los aspectos de usabilidad que propone el NIST en su publicación SP-800-63.

Palabras clave:

- **CIBERSEGURIDAD**
- **CONTRASEÑAS GRÁFICAS**
- **CIBERSEGURIDAD**
- **AUTENTICACIÓN**

Abstract

Nowadays the digital information is one of the most important resources of people and companies, the cybercrime is presented as a problem because it is dedicated to the subtraction of this resource and has been increasing over the years, therefore is essential to implement in the computer systems strategies that mitigate data theft, in view of this reality the present study aims to propose a hybrid authentication system, to group the advantages of graphic passwords and single passwords, proposing an alternative authentication mechanism based on disposable graphic passwords, supported by an algorithm that generates randomic sequences, validated by the streak test that verifies the randomness of sequences of sequences and evaluated against theft attacks of credentials such as Keylogger, brute force or dictionary attack and shoulder Surf which are presented as simple techniques of application For the theft of credentials, you can carry out a usability evaluation process where 92% acceptance of the proposed mechanism is reflected, the scheme must take into account the good practices and usability aspects proposed by the NIST in its publication SP -800-63.

Keywords:

- **CYBER SECURITY**
- **GRAPHIC PASSWORDS**
- **CYBER SECURITY**

  AUTHENTICATION