RESUMEN

El proceso de encriptación es muy importante para diversas aplicaciones que abarque el tratamiento de información sensible ya que permite proteger de agentes externos la información almacenada en bases de datos, brindando seguridad y confianza al usuario. El modelo de encriptación de curva elíptica presenta como ventaja una generación de claves más cortas pero al mismo nivel de seguridad que otros métodos con longitudes de claves mucho más extensas. El proyecto implementa un sistema de encriptación utilizando el algoritmo de curva elíptica para protección de la información de una base datos ante ataques desde un dispositivo móvil. Se diseñó la interfaz de ingreso de información a la base de datos desde donde se realiza proceso de encriptación y desencriptación, de tal manera que en el gestor de base de datos se almacene la información de usuario encriptada. La aplicación de la norma ISO/IEC 27001 permite establecer una correcta gestión de la seguridad de la información, mediante controles y estrategias basados en el ciclo de mejora continua. Finalmente, el sistema fue sometido a pruebas de validación de seguridad de la información cuando se accede a ella desde un dispositivo móvil y se transmite la información por un canal inseguro, realizando el número necesario de pruebas para garantizar que la información viaja a través de la red está encriptada, siendo ilegible para el intruso incluso si logra tener acceso a ella.

PALABRAS CLAVES:

- **ENCRIPTACIÓN DE CURVA ELÍPTICA**
- **GESTOR DE BASE DE DATOS**
- **ISO/IEC 27001**

ABSTRACT

The encryption process is very important for various applications that cover the treatment of sensitive information since it allows the protection of information stored in databases from external agents, providing security and trust to the user. The elliptic curve encryption model has the advantage of generating shorter keys but at the same level of security as other methods with much longer key lengths. The project implements an encryption system using the elliptic curve algorithm to protect the information in a database against attacks from a mobile device. The interface for entering information into the database from which the encryption and decryption process is carried out was designed, so that the encrypted user information is stored in the database manager. The application of the ISO / IEC 27001 standard allows the correct management of information security to be established, through controls and strategies based on the continuous improvement cycle. Finally, the system was subjected to information security validation tests when it is accessed from a mobile device and the information is transmitted through an insecure channel, performing the necessary number of tests to ensure that the information travels through the network is encrypted, being unreadable to the intruder even if you can access it.

KEYWORDS:

- **ELLIPTIC CURVE CRYPTOGRAPHY**
- **DATABASE MANAGERX**
- **ISO/IEC 27001**