**Introducción**

En el mundo interconectado de hoy, la necesidad de mantener la seguridad de información o propiedad física, se está volviendo cada vez más importante y cada vez más difícil. De vez en cuando escuchamos sobre los delitos de fraude con tarjetas de crédito, intrusión informática por piratas informáticos o violaciones de seguridad en una empresa o edificio gubernamental. En la mayoría de estos delitos, los delincuentes se aprovechaban de una falla fundamental en los sistemas de control de acceso convencionales: los sistemas no otorgan acceso por "quienes somos", sino por "lo que tenemos", como tarjetas de identificación, claves, contraseñas, PIN, etc. Ninguno de estos medios realmente nos define. Más bien, son simplemente un medio para autenticarnos. No hace falta decir que, si alguien roba, duplica o adquiere estos medios de identidad, podrá acceder a nuestros datos o nuestra propiedad personal en cualquier momento querer. Recientemente, la tecnología estuvo disponible para permitir la verificación de la identidad individual "verdadera". Esta tecnología se basa en un campo llamado "biometría". El control de acceso biométrico es métodos automatizados para verificar o reconocer la identidad de una persona viva sobre la base de algunas características fisiológicas, como huellas dactilares o rasgos faciales, o algunos aspectos del comportamiento de la persona, como su estilo de escritura a mano o patrones de pulsación de teclas. Dado que los sistemas biométricos identifican a una persona por características biológicas, son difíciles de falsificar. Entre los diversos métodos de identificación biométrica, el fisiológico. Los métodos (huella dactilar, rostro, ADN) son más estables que los métodos en la categoría de comportamiento (pulsación de tecla, impresión de voz). La razón es que las características fisiológicas a menudo no se pueden alterar excepto por una lesión grave. Los patrones de comportamiento, por otro lado, puede fluctuar debido al estrés, la fatiga o la enfermedad. Sin embargo, las identificaciones de comportamiento tienen la ventaja de no ser intrusivas.

**Objetivos**

- Brindar un mayor nivel de seguridad.

-Registrar y almacenar los datos de todos los individuos que ingresen (residentes,visitantes,etc).

- Facilitar el ingreso a los inquilinos u empleados.  
  
-Evitar la exposición del personal de seguridad designado a peligros (robo o asalto).  
  
-Evitar el ingreso a desconocidos.

**Especificación de requerimientos del sistema**

* Cámaras
* Computadoras
* Software

**Procedimiento de instalación y pruebas**

**Arquitectura del software**

**Descripción de procesos**

**Especificación API**

**Aspectos relevantes**