**Marco Teórico**

**1. Seguridad y Control de Acceso**

En el contexto actual, la protección de la información y el control de acceso a zonas restringidas son aspectos críticos en empresas y organizaciones. Los sistemas de seguridad tradicionales basados en llaves o tarjetas han mostrado vulnerabilidades frente a métodos de falsificación o robo. Por ello, se ha impulsado el uso de tecnologías más avanzadas, como los sistemas biométricos, que permiten autenticar a los usuarios basándose en características físicas únicas (como huellas dactilares), elevando así el nivel de seguridad.

**2. Biometría y Sistemas de Reconocimiento**

La biometría es la ciencia que se encarga del reconocimiento de individuos a partir de sus rasgos biológicos o de comportamiento con el fin de poder identificar al individuo que desee acceder a él y su identidad. Además, cada individuo tiene características únicas y pese a eso, se pueden utilizar para identificarlo.

* **Características Biométricas:** Esto incluye la huella dactilar. Este elemento posee una singularidad que dificulta su duplicación, haciendo que no cualquier usuario pueda acceder a ella sin que esta tenga los mismos rasgos de la otra persona, lo que lo convierte en métodos fiables para la autenticación del personal autorizado y que solo él pueda acceder a los datos biométricos que registró.
* **Ventajas del Acceso Biométrico:** Tiene mayor seguridad al reducir el riesgo de falsificación y de compartimiento, las huellas dactilares no se pueden copiar, dando ventaja a la unicidad y mejora en la seguridad. por lo tanto, una persona no puede copiar sus mismos rasgos para poder acceder al sistema, y la comodidad de no requerir memorizar contraseñas de ningún tipo y la rapidez en la identificación del usuario. solo se debe registrar la huella dactilar y queda guardada en el registro para que así, el lector de huellas reconozca la huella del usuario.
* **Desafíos:** Aspectos como la precisión de los sensores, calibrarlos y estabilizarlos de una buena manera para que el reconocimiento sea efectivo y el personal autorizado no tenga dificultades en acceder a la información confidencial de la empresa, tener condiciones ambientales adecuadas para que esta herramienta funcione de la mejor manera protegiendo los circuitos en una forma en la que la humedad o externos lo dañen y la necesidad de procesamiento de datos en tiempo real, registrar los accesos y salidas del personal autorizado y el tiempo en el que estuvo dentro de ese acceso pueden influir en el desempeño del sistema.

**3. Microcontroladores y Arduino**

El uso de microcontroladores es fundamental en el desarrollo de sistemas embebidos para aplicaciones de seguridad ya que con los microcontroladores podemos realizar pruebas de programación y de que estos mismos funcionen según las ordenes que les demos.

* **Arduino:** Es una plataforma de prototipado electrónico de código abierto que facilita la integración de hardware y software en proyectos, una placa electrónica con un microcontrolador programable que se utiliza para interactuar con el mundo físico, utilizando sensores y actuadores.
  + **Arquitectura:** Basada en microcontroladores programables, Arduino permite la conexión de diversos sensores y actuadores, posibilitando la creación de sistemas interactivos y personalizados y creación de sistemas de automatización para el hogar, la industria o la agricultura. placa basada en un microcontrolador ATMEL. Los microcontroladores son circuitos integrados en los que se pueden grabar instrucciones, las cuales se escriben con el lenguaje de programación que puedes utilizar en el entorno Arduino IDE.
  + **Aplicaciones en Seguridad:** Gracias a su flexibilidad y comunidad de apoyo, se ha empleado en múltiples proyectos de automatización y control, como sistemas de acceso y monitoreo en tiempo real y modificar las configuraciones implementadas cuando sea necesario.

**4. Integración de Sensores Biométricos con Arduino**

La integración de sensores biométricos en un sistema basado en Arduino implica la conexión y configuración de dispositivos que capturan datos biológicos.

* **Sensor Biométrico:** El componente encargado de capturar la información (por ejemplo, una huella digital) debe ser compatible con Arduino. de lo contrario este no funcionara en el Arduino
* **Procesamiento de Datos:** El microcontrolador procesa la información capturada para compararla con una base de datos preestablecida, determinando si el usuario está autorizado a acceder.
* **Interacción con Actuadores:** Una vez verificada la identidad, el sistema puede activar un actuador (como un relé) que permita o deniegue el acceso a la zona restringida.

**5. Consideraciones de Implementación y Seguridad**

La implementación de un sistema de seguridad biométrico no solo requiere una correcta integración técnica, sino también el manejo seguro de la información:

* **Protección de Datos:** Es fundamental emplear técnicas de cifrado y almacenamiento seguro para evitar la exposición de los datos sensibles de los usuarios.
* **Confiabilidad del Sistema:** El diseño debe contemplar redundancias y mecanismos de alerta en caso de fallos o intentos de acceso no autorizados y que quede en el registro los errores.
* **Identificar riesgos:** Determinar los peligros y vulnerabilidades de los sistemas y datos registrados.
* **Evaluar los riesgos:** Analizar la probabilidad y el impacto de cada riesgo identificado.
* **Establecer medidas de control:** Implementar mecanismos para mitigar o eliminar los riesgos que se puedan presentar.