**SENA**

**CENTRO PARA LA INDUSTRIA DE LA COMUNICACIÓN GRAFICA**

**TECNICO EN SISTEMAS TELEINFORMATICOS**

**“SISTEMA DE SEGURIDAD BIOMETRICO”**

**MARCO TEORICO**

Presenta:

**ADRIAN FELIPE ROJAS FRAILE**

**CARLOS ARTURO ZAMBRANO QUITIAN**

**DANIEL JOSE SERRANO PALENCIA**

Director de ficha:

**OSVALDO PEREZ**

Bogotá, Colombia Abril, 2025

Tabla de contenido

[**INTRODUCCIÓN** 3](#_Toc196767544)

[MARCO TEORICO 4](#_Toc196767545)

[1. QUE ES UN CONTROL DE SEGURIDAD DE ACCESO 4](#_Toc196767546)

[2. ¿QUÉ ES SEGURIDAD BIOMETRICA? 4](#_Toc196767547)

[4. ¿QUE TIPO DE SEGURIDAD BIOMETRICA SE USARÁ? 4](#_Toc196767548)

[ VENTAJAS DEL ACCESO BIOMÉTRICO 5](#_Toc196767549)

[ DESVESTANJAS DEL ACCESO BIOMETRICO 5](#_Toc196767550)

[5. INTEGRACIÓN DE SENSORES BIOMÉTRICOS CON ARDUINO 6](#_Toc196767551)

[6. CONSIDERACIONES DE IMPLEMENTACIÓN Y SEGURIDAD 6](#_Toc196767552)

[7. DESAFÍOS 6](#_Toc196767553)

[8. CIBERSEGURIDAD EN EL CONTROL DE ACCESO BIOMETRICO 7](#_Toc196767554)

[9. LEY SOBRE LOS DATOS PERSONALES Y SENSIBLES 7](#_Toc196767555)

[REFERENCIAS 8](#_Toc196767556)

# **INTRODUCCIÓN**

Actualmente, la protección de la información y el control de acceso a zonas restringidas son las necesidades de una empresa. Los sistemas de seguridad tradicionales como los son las llaves o tarjetas han mostrado inseguridad frente a métodos de falsificación, robo o perdida de la llave o tarjeta. Por dicho problema, proponemos el uso de tecnologías más avanzadas, como los sistemas biométricos, que permiten autenticar a los usuarios basándose en características físicas únicas (como huellas dactilares, reconocimiento facial), o en última instancia el uso de contraseña, elevando así el nivel de seguridad.

**Objetivo General**

Crear un sistema de seguridad biométrico basado en Arduino para el control de acceso a una sala Restringida dentro de una empresa, permitiendo el ingreso únicamente a personal autorizado Mediante el uso de reconocimiento biométrico, con el fin de proteger información confidencial y Garantizar la seguridad del área.

**Objetivos Específicos**

1. Diseñar y ensamblar el sistema de control de acceso: Utilizando una placa Arduino, un Sensor biométrico y una cerradura electrónica para permitir la autenticación segura.
2. Programar el software del sistema: En Arduino IDE se realizará toda la programación necesaria para el buen funcionamiento del proyecto, se llevará a cabo la configuración necesaria para el sistema de seguridad biométrico (sensor de huellas dactilares).
3. Realizar base de datos: Aquí se llevará a cabo el registro de las personas que ingresen a el área restringida y así tener un seguimiento del usuario (Hora de ingreso, hora de salida, Documento de identidad, que cargo tiene en la empresa etc.)
4. Implementar medidas de seguridad adicionales: Como almacenamiento cifrado de datos Biométricos y un sistema de respaldo en caso de fallos eléctricos o errores en la Autenticación.

## MARCO TEORICO

### 1. **QUE ES UN CONTROL DE SEGURIDAD DE ACCESO**

Es una técnica de seguridad que regula quién puede ver, usar o acceder a ciertos recursos dentro de una organización. Este proceso de seguridad garantiza que las áreas, datos y sistemas sensibles solo estén disponibles para usuarios autorizados.

Aspectos clave del control de acceso:

* **Control de acceso físico:** este administra el ingreso a ubicaciones físicas mediante herramientas como cerraduras, dispositivos biométricos o tarjetas de acceso.
* **Control de acceso lógico:** administra las conexiones a sistemas digitales, incluido el acceso a datos, aplicaciones y redes.

### 2. ¿QUÉ ES SEGURIDAD BIOMETRICA?

La seguridad biométrica es la que se encarga del reconocimiento de individuos a partir de sus rasgos biológicos, con el fin de poder identificar al individuo que desee acceder a una zona restringida de solo personal autorizado y verificar su identidad. Y este sistema es seguro debido a que cada individuo autorizado cuenta con características únicas, que se pueden utilizar para identificarlo.

### **¿QUE TIPO DE SEGURIDAD BIOMETRICA SE USARÁ?**

### **Biometría fisiológica**

Emplea atributos físicos, estructurales y relativamente estáticos de una persona, como sus huellas dactilares, el patrón del iris, los contornos del rostro o la geometría de las venas de las manos. Algunas modalidades son microscópicas, pero aun así presentan estructuras biológicas y químicas que pueden adquirirse e identificarse.

Muchos datos biométricos fisiológicos son características permanentes y resistentes al cambio, a menos que se dañen, degraden o destruyan accidental o intencionalmente. Ejemplos de ello, en el caso de las huellas dactilares, podrían incluir la erosión parcial de las crestas de fricción en las manos de quienes manipulan o colocan ladrillos durante largos periodos, la pérdida o amputación de manos o dedos y, en casos extremos, la cirugía invasiva o la autolesión para eliminar o alterar la estructura de las crestas.

### VENTAJAS DEL ACCESO BIOMÉTRICO

 **SEGURIDAD SUPERIOR:** Las características biométricas son únicas por individuo, lo

que dificulta significativamente la suplantación de identidad y el acceso no autorizado.

** COMODIDAD:** Los usuarios no necesitan recordar contraseñas ni portar tarjetas; la autenticación es rápida y sencilla.

 **PRECISIÓN:** Los sistemas modernos ofrecen alta precisión en la verificación de identidad, minimizando errores.

 **REDUCCIÓN DE COSTOS A LARGO PLAZO:** Disminuyen gastos asociados a la gestión de tarjetas y reemplazo de contraseñas.

 **INTRANSFERIBILIDAD:** Los rasgos biométricos están ligados a la persona y no se pueden perder, compartir ni robar fácilmente.

 **A PRUEBA DE SUPLANTACIÓN:** Requieren la presencia física del usuario al momento de la autenticación.

### DESVENTAJAS DEL ACCESO BIOMETRICO

 **VULNERABILIDADES DE SEGURIDAD:** Aunque seguros, no son inmunes a ataques o fallos en el sistema.

 **IRREVERSIBILIDAD DE LOS DATOS:** Si una base de datos se compromete, la información biométrica robada es permanente.

 **POSIBLES ERRORES:** Pueden ocurrir falsos positivos o negativos debido a la tecnología, cambios físicos o factores ambientales.

 **DEPENDENCIA TECNOLÓGICA:** Fallos eléctricos o en los dispositivos pueden impedir la autenticación.

 **LIMITACIONES EN CIERTOS ENTORNOS:** No siempre son ideales en lugares con alta rotación de personal o condiciones que afecten las características biométricas.

 **RIESGO DE ROBO DE DATOS:** Existe la posibilidad de que las bases de datos biométricas sean vulneradas.

 **POSIBILIDAD DE FALSIFICACIÓN:** Aunque difícil, los rasgos biométricos podrían ser falsificados.

 **PROBLEMAS DE ACCESIBILIDAD:** Algunos sistemas pueden no funcionar bien en ciertas condiciones ambientales o para personas con ciertas discapacidades.

### 5. 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 del individuo

* **SENSOR BIOMÉTRICO:** El componente encargado de capturar la información (por ejemplo, una huella digital, reconocimiento facial) debe ser compatible con Arduino. de lo contrario este no funcionara en el Arduino
* **VERIFICACIÓN DEL INDIVIDUO:** Una vez verificada la identidad del individuo, dará o no el acceso a la zona restringida.

### 6. 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.

### 7. 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 lo dañen, registrar los accesos y salidas del personal autorizado y el tiempo en el que estuvo dentro de ese acceso.

### 8. CIBERSEGURIDAD EN EL CONTROL DE ACCESO BIOMETRICO

La ciberseguridad es el conjunto de prácticas y tecnologías destinadas a proteger los sistemas, redes y datos contra accesos no autorizados, ataques o daños. En nuestro sistema de acceso mediante seguridad biométrica, la ciberseguridad juega un papel fundamental: al momento de que un usuario accede a una zona restringida, su identidad se verifica contra una base de datos protegida. Esta base de datos almacena de forma segura la información personal y biométrica de cada usuario, utilizando mecanismos de cifrado y protocolos de seguridad avanzados, garantizando que la información no pueda ser alterada, robada o expuesta a terceros. De este modo, aseguramos no solo la autenticación correcta del individuo, sino también la protección de su información personal conforme a las mejores prácticas y normativas de seguridad.

### 9. LEY SOBRE LOS DATOS PERSONALES Y SENSIBLES

**Artículo 6° Ley 1581 de 2012. Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:**

1. El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
2. El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
3. El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
4. El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
5. El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares**.**

### 

### REFERENCIAS

<https://www.deltaprotect.com/blog/controles-de-acceso-que-son-y-por-que-son-importantes-para-proteger-tu-empresa>

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

<https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/>