Documento de Requerimientos para el Sistema de Seguridad Basado en Huella Dactilar

Integrantes:
- Juan Camilo Dueñas
- Keily Pinzón
- Andrés Prada Sandoval

1. Introducción

Este proyecto propone la implementación de un sistema de control de acceso mediante reconocimiento de huella dactilar en la entrada de la Universidad. El objetivo es garantizar que solo estudiantes, personal y personas autorizadas tengan acceso a las instalaciones, reduciendo la entrada de individuos no relacionados que puedan generar conflictos.

2. Objetivos del sistema

- **Objetivo principal**: Proveer un sistema de control de acceso eficiente, seguro y fácil de utilizar, basado en la autenticación biométrica de huellas dactilares.
- **Objetivos específicos**:
    - Aumentar la seguridad en la entrada de la universidad.
    - Garantizar que solo personas autorizadas puedan acceder a las instalaciones.
    - Minimizar el riesgo de fraudes y el uso no autorizado de tarjetas de acceso.
    - Facilitar la gestión y monitoreo del acceso a través de una plataforma centralizada.

---

3. Requerimientos Funcionales

3.1. Autenticación de usuarios mediante huella dactilar

- El sistema debe permitir que los usuarios (estudiantes y personal) puedan registrar su huella dactilar en una base de datos central.
- El sistema debe autenticar a cada persona que intente ingresar verificando su huella contra las huellas registradas en la base de datos.
- El sistema debe rechazar el acceso a personas cuya huella no esté registrada.

3.2. Registro y gestión de usuarios

- El sistema debe contar con una interfaz para que el personal administrativo registre y gestione a los usuarios.
- El sistema debe permitir el registro de nuevas huellas para estudiantes y personal autorizado, con la capacidad de asignar roles (estudiante, profesor, visitante).
- El sistema debe permitir la eliminación o actualización de los registros cuando sea necesario (por ejemplo, cuando un estudiante se gradúe).

3.3. Control de acceso en tiempo real

- El sistema debe registrar cada acceso con la fecha, hora y el usuario correspondiente.
- El sistema debe permitir la consulta de registros históricos de accesos para auditorías o análisis de seguridad.
- Debe haber un sistema de alertas que notifique si se intentan varios accesos fallidos consecutivos por una misma persona o dispositivo.

3.4. Integración con sistemas de monitoreo

- El sistema debe integrarse con cámaras de seguridad que monitoreen la entrada, activándose automáticamente si un acceso es denegado o si se detecta un comportamiento sospechoso.

---

4. Requerimientos No Funcionales

4.1. Seguridad

- La información biométrica (huellas dactilares) debe almacenarse en un formato encriptado y debe estar protegida para evitar accesos no autorizados o filtraciones de datos.
- El sistema debe cumplir con las normativas de protección de datos personales y privacidad, garantizando que la información recolectada solo sea utilizada para los fines previstos.

4.2. Escalabilidad

- El sistema debe ser capaz de gestionar más de 30,000 usuarios sin comprometer el rendimiento.
- El tiempo de autenticación no debe exceder los 2 segundos por persona, incluso en horas pico.

4.3. Disponibilidad

- El sistema debe tener una disponibilidad del 99.9%, garantizando que esté operativo en todo momento para no afectar el acceso a la universidad.
- Debe contar con un sistema de respaldo (failover) en caso de fallos del sistema principal.

4.4. Mantenimiento y soporte

- El sistema debe ser fácil de mantener y actualizar por el personal técnico de la universidad.
- Debe contar con documentación clara para facilitar su administración y posibles futuras expansiones.

4.5. Usabilidad

- La interfaz del sistema debe ser intuitiva y fácil de usar tanto para el personal administrativo como para los usuarios que registren sus huellas.
- Los dispositivos de reconocimiento de huella dactilar deben ser accesibles y funcionales en todo momento, garantizando su uso incluso en condiciones de suciedad o humedad.

4.6. Rendimiento

- El sistema debe ser capaz de procesar múltiples accesos simultáneamente sin disminuir su velocidad ni eficiencia.
- El sistema debe garantizar que los registros de acceso se actualicen en tiempo real.

---

5. Información adicional

5.1. Beneficios del uso de la huella dactilar

- **Seguridad**: Las huellas dactilares son únicas para cada individuo, lo que reduce significativamente el riesgo de fraude.
- **Eficiencia**: A diferencia del reconocimiento facial o las tarjetas de acceso, el uso de la huella dactilar es más rápido y menos propenso a fallos por factores externos (como cambios en la apariencia o pérdida de tarjetas).
- **Costos**: Aunque los dispositivos de lectura de huella pueden tener un costo inicial, a largo plazo son más económicos que mantener sistemas basados en tarjetas o en reconocimiento facial.

5.2. Limitaciones potenciales

- **Suciedad o desgaste**: Los dispositivos de huella dactilar pueden presentar fallos si las huellas están sucias o si los dispositivos no reciben el mantenimiento adecuado.
- **Interrupciones del servicio**: Es crucial tener planes de contingencia para que el acceso no se vea comprometido en caso de fallos en el sistema o en la energía eléctrica.