Actividad 2: Fase de Diseño

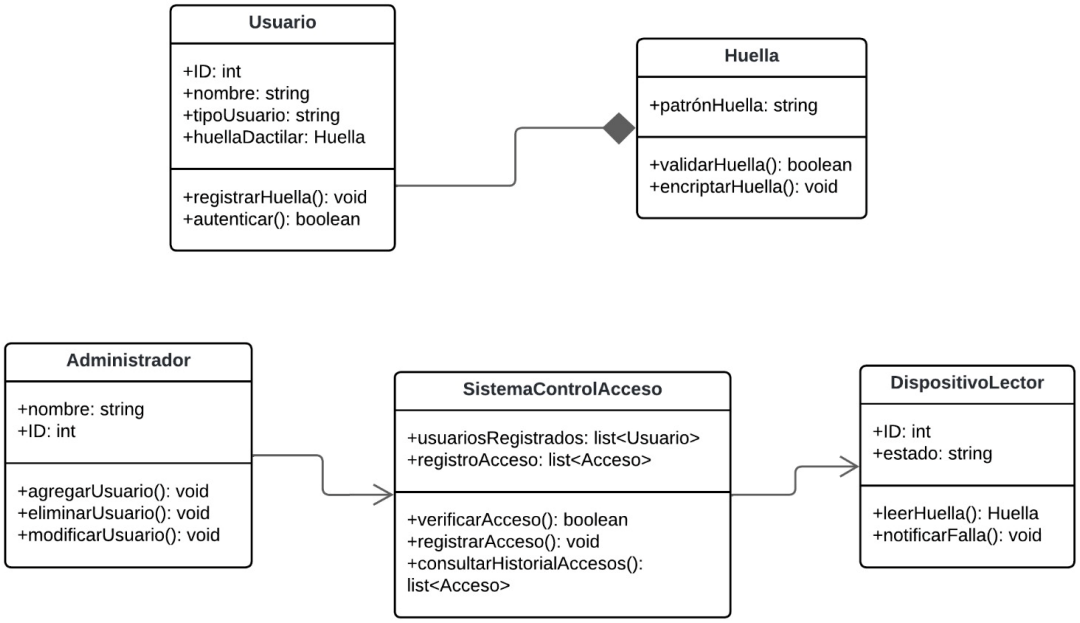
Integrantes:

Juan Camilo Dueñas

Keyly Katherine Pinzon

Andrés Prada Sandoval

1. Diagrama de clases



Relaciones:

Usuario - Huella: Existe una relación de composición entre Usuario y Huella, ya que cada usuario tiene una huella asociada, que es esencial para el proceso de autenticación.

Administrador - SistemaControlAcceso: El administrador gestiona el sistema, lo que le permite agregar, eliminar o modificar usuarios.

SistemaControlAcceso - DispositivoLector: El sistema se comunica con el lector para capturar las huellas y verificar su validez antes de permitir el acceso.

2. **Esquema de Arquitectura del Sistema:**

   El sistema de seguridad basado en huella dactilar tiene una arquitectura cliente-servidor con los siguientes componentes:

Dispositivo Lector de Huellas:

- Captura la huella dactilar y la envía al sistema para su verificación.
- Se conecta con el servidor a través de una red local.

Servidor Central

- Procesa las solicitudes de autenticación comparando las huellas capturadas con la base de datos.
- Almacena de forma segura los datos biométricos en una base de datos encriptada.

Base de Datos:

- Contiene los datos de los usuarios y sus huellas en formato encriptado.
- Registra los eventos de acceso para auditorías y análisis de seguridad.

Interfaz de Usuario:

- Permite al personal administrativo gestionar usuarios (registro, eliminación, modificación).
- Permite la consulta de los registros de acceso en tiempo real.

Interacción de componentes:

1. El Dispositivo Lector captura la huella del usuario.

2. El lector envía la información al Servidor, que verifica la huella con los registros en la Base de Datos.

3. El Servidor responde al Dispositivo para permitir o denegar el acceso, y registra el evento.

4. Los administradores pueden utilizar la Interfaz de Usuario para gestionar usuarios o consultar registros.

3. **Justificación del Diseño:**

Decisiones de Diseño:

- **Tecnologías:** Se utilizarán lectores de huellas compatibles con los principales sistemas operativos y servidores centralizados para garantizar la escalabilidad y la gestión de miles de usuarios.

- **Base de datos:** El sistema usará una base de datos SQL debido a la necesidad de consultas rápidas y capacidad para manejar registros históricos. La información sensible se almacenará de forma encriptada.
- **Interfaces de usuario:** El sistema contará con una interfaz gráfica intuitiva para facilitar la gestión por parte del personal administrativo.

Consideraciones de Seguridad:

- **Encriptación:** Se implementará en la base de datos para asegurar la protección de los datos biométricos y evitar suplantaciones o filtraciones.

- **Monitoreo:** El sistema estará equipado con alertas ante intentos de acceso fallidos consecutivos, así como integración con cámaras de seguridad para evitar el acceso no autorizado.

Conclusión:

El diseño del sistema de seguridad basado en huella dactilar se fundamenta en la necesidad de garantizar un control de acceso eficiente y seguro para entornos como instituciones educativas. Las decisiones tecnológicas, como el uso de bases de datos encriptadas y sistemas biométricos, se tomaron para asegurar tanto la privacidad de los usuarios como la integridad de los datos almacenados. Además, se consideraron aspectos de usabilidad y escalabilidad, lo que permite que el sistema gestione grandes volúmenes de usuarios sin comprometer el rendimiento. Las funcionalidades de monitoreo y respaldo aseguran que el sistema se mantenga operativo incluso ante posibles fallos, garantizando así una solución robusta y confiable para el control de acceso.