AVANCE PROYECTO FINAL SISTEMA “NEOCDT”

INTEGRANTES:

- SAMUEL SALAZAR TRUJILLO – 2232061
- ROIMAN URREGO ZUÑIGA – 2231385
- ISABELA CABEZAS OBREGÓN – 2226013
- ISABELLA ORTÍZ HERNANDEZ – 2226215
- SEBASTIAN BUSTAMANTE LOPEZ – 2230843

DOCENTE:

RODRIGO ESCOBAR LOPEZ

ASIGNATURA:

INGENIERIA DE SOFTWARE 2

UNIVERSIDAD AUTONOMA DE OCCIDENTE
PERIODO 2025 – 2
CALI - VALLE

CONTEXTO

NeoBank, como banco 100% digital en LATAM, busca optimizar la experiencia de sus clientes mediante el módulo NeoCDT**,** orientado a la apertura y gestión de Certificados de Depósito a Término de manera totalmente digital. Actualmente existen problemas de fricción en el registro, falta de visibilidad en el estado de las solicitudes, operaciones manuales y debilidades en seguridad y calidad del software.

Frente a esta situación, se identificaron los requisitos funcionales y no funcionales que el sistema debe cumplir, priorizados con la técnica MoSCoW**,** con el fin de asegurar un desarrollo alineado a los objetivos del negocio y a las necesidades de los usuarios.

REQUISITOS FUNCIONALES

ID	Requisito	Impacto en la solución	Objetivo asociado	Moscow
RF1	El sistema debe permitir abrir CDTs de forma totalmente digital, sin necesidad de trámites presenciales.	Facilita la inclusión financiera y atrae clientes que buscan procesos ágiles.	Flujo centralizado para solicitudes de CDT.	Must Have
RF2	El sistema debe reutilizar la información ya registrada del cliente (KYC), evitando solicitarla de nuevo.	Reduce fricción, errores y mejora la experiencia de uso.	Reducción de fricción en login y registro.	Must Have
RF3	El sistema debe mostrar al cliente, en tiempo real, el estado de su solicitud (borrador, en validación, aprobada, rechazada, cancelada).	Aporta transparencia, confianza y control al cliente.	Transparencia de estados y trazabilidad.	Must Have
RF4	El sistema debe permitir al cliente renovar su CDT de forma automática o manual según prefiera.	Favorece la fidelización y retención de clientes.	Flujo centralizado y trazabilidad.	Should Have

RF5	El sistema debe ofrecer un panel para que los agentes bancarios gestionen y supervisen todas las solicitudes.	Disminuye la operación manual y mejora la eficiencia interna.	Flujo centralizado y operación eficiente.	Must Have
RF6	El sistema debe permitir al cliente cancelar su solicitud de CDT mientras esté en estado de borrador o validación.	Da flexibilidad y mayor control sobre sus decisiones.	Flujo centralizado y experiencia de usuario.	Should Have
RF7	El sistema debe permitir a los administradores consultar reportes y métricas sobre CDTs (aperturas, renovaciones, cancelaciones).	Mejora la toma de decisiones y el control de calidad.	Métricas y calidad del sistema.	Could Have

REQUISITOS NO FUNCIONALES

ID	Requisito	Categoría	Especificación (cómo se mide / aplica)	Prioridad (MoSCoW)	Justificación
RNF1	El sistema debe encriptar toda la información del cliente, tanto en almacenamiento como en transmisión.	**Seguridad**	Uso obligatorio de **TLS 1.3** en transmisión y **AES-256** en la base de datos.	Must Have	Es obligatorio en un banco digital para proteger datos sensibles y cumplir la ley.

RNF2	El sistema debe implementar autenticación multifactor (MFA) en operaciones sensibles.	**Seguridad**	Confirmación de operaciones mediante **OTP, biometría o token digital**.	Must Have	Evita fraudes y accesos indebidos.
RNF3	El sistema debe garantizar la disponibilidad del servicio de manera continua.	**Disponibilidad**	Uptime mínimo del **99.5% mensual** con redundancia en servidores.	Must Have	Los clientes esperan acceder a su dinero en todo momento.
RNF4	El sistema debe responder en tiempos adecuados a las acciones del cliente.	**Rendimiento**	Consultas y aperturas de CDTs deben resolverse en **máx. 3 segundos**.	Should Have	Mejora la experiencia del usuario, aunque puede optimizarse con el tiempo.
RNF5	El sistema debe soportar picos de uso altos sin degradar su rendimiento.	**Escalabilidad**	Manejo de al menos **10.000 usuarios concurrentes**.	Should Have	Garantiza estabilidad en campañas o temporadas de alta demanda.
RNF6	El sistema debe contar con pruebas automatizadas de calidad integradas al pipeline.	**Calidad del software**	Cobertura mínima del **80% en pruebas unitarias** dentro de CI/CD.	Must Have	Reduce errores en producción y asegura confiabilidad.
RNF7	El sistema debe registrar y auditar todas las operaciones realizadas por los usuarios.	**Seguridad / Auditoría**	Guardar usuario, fecha, acción y resultado en un **log seguro** durante mínimo 5 años.	Must Have	Necesario para cumplir regulaciones y auditorías financieras.

HISTORIAS DE USUARIO

1. **Feature:** Abrir un CDT
   Como cliente ***quiero*** poder abrir un CDT de manera digital ***para*** evitar largas filas y tiempos de espera.
   - **Scenario:** Apertura exitosa de un CDT

   Given el cliente inicia sección en el sistema
   And encuentra el módulo “abrir nuevo CDT”
   When completa los datos requeridos
   Then el sistema registra la solicitud en estado “Pendiente por aprobación”
   And el sistema muestra el mensaje “Solicitud de apertura de CDT exitoso”

2. **Feature:** Registro de cliente nuevo
   Como cliente nuevo ***quiero*** poder registrar mis datos a una cuenta ***para*** gestionar nuevas solicitudes de CDT.
   - **Scenario:** Registro exitoso

   Given el cliente quiere abrir un CDT
   And no tiene una cuenta vigente en el sistema
   When ingresa todos los datos personales requeridos para el registro
   Then el sistema crea una cuenta de usuario
   And el usuario recibe un correo de confirmación de apertura de cuenta

3. **Feature:** Uso de datos registrados previamente
   Como cliente ***quiero*** utilizar los datos ya registrados en el sistema sin la necesidad de repetir estos al momento de acceder o abrir un CDT, ***para*** evitar réplicas de información y realizar pasos innecesarios.
   - **Scenario:** Reutilizacion de datos ya registrados

   Given el cliente inicia sesión en el sistema
   When el cliente da click en “acceder a mi CDT”
   Then el sistema carga automáticamente los datos ya registrados en el perfil del usuario

4. **Feature:** Estado de las solicitudes
   Como cliente ***quiero*** tener claridad sobre el estado de mi solicitud del CDT ***para*** poder tener un mayor entendimiento y transparencia en el proceso.
   - **Scenario:** Visualización del estado de la solicitud

   Given el cliente inicia sesión en su cuenta
   When da click en el apartado de “Mis solicitudes”
   Then el sistema muestra una lista con las solicitudes del cliente junto con su estado actual (Pendiente, Aprobado, Rechazado, Cancelado).

5. **Feature:** Renovación de CDTs
   Como cliente ***quiero*** poder renovar mi CDT de forma manual o automática según mis preferencias, ***para*** asegurar mis inversiones.
   - **Scenario:** Renovación automatizada

Given el cliente tiene un CDT con fecha próxima a vencer
And tiene activa la opción de “renovar automáticamente”
When llega la fecha de vencimiento del CDT
Then el sistema genera una nueva solicitud de CDT con los datos previamente registrados.

6. **Feature:** Panel de Visualización de agente
   Como agente ***quiero*** tener un panel centralizado donde tenga acceso a la visualización completa de todas las solicitudes, ***para*** así reducir procesos manuales.
   ❖ **Scenario:** Acceso al panel de visualizaciones
   Given el agente inicia sesión en el sistema
   When el agente accede al panel
   Then el sistema despliega una lista de todas las solicitudes de CDT

7. **Feature:** Cancelación de solicitud de CDT
   Como cliente ***quiero*** poder cancelar mi solitud de CDT mientras esta esté en estado de borrado o validación ***para*** tener control sobre mis decisiones.
   ❖ **Scenario:** Cancelación de solicitud pendiente por aprobación
   Given el cliente tiene una solicitud en estado “Pendiente por aprobación”
   When hace click en la opción “Cancelar Solicitud”
   Then el sistema debe cambiar el estado de la solicitud a “cancelado”

8. **Feature:** Consulta de reportes
   Como administrador ***quiero*** poder consultar los reportes y las métricas de las solicitudes de CDT activas ***para*** así tener un análisis completo del producto y tomar decisiones.
   ❖ **Scenario:** Consulta de reportes de CDTs
   Given el administrador inicia sesión en el sistema
   And accede al panel de control
   When selecciona la opción de “ver reportes”
   Then el sistema despliega estadísticas de CDTs pendientes por aprobación, activos, renovados y cancelados.

ATRIBUTOS – ESCENARIOS DE CALIDAD

De acuerdo con el contexto, hemos identificado los atributos más relevantes:

1. **Seguridad:** El sistema NeoCDT maneja información muy sensible como lo son datos personales de los clientes y su dinero en los CDT. Si la seguridad es débil, el riesgo no es solo que un atacante robe información o dinero, sino también que el banco enfrente problemas legales, pérdida de reputación y pérdida de confianza de los usuarios. Además, el mismo contexto indica que no existen análisis estáticos ni pruebas de seguridad, lo que significa que las vulnerabilidades podrían llegar fácilmente a producción sin ser detectadas.

2. **Usabilidad:** El primer contacto de los usuarios con el sistema es el proceso de apertura de un CDT. En el contexto se dice que actualmente es un proceso engorroso, pues los clientes deben repetir información ya que el sistema no reconoce cuando ya hay datos previos y el flujo es poco claro. Esto provoca abandono (clientes que nunca terminan el registro), genera frustración y aumenta la carga manual de los agentes para corregir o validar solicitudes.

3. **Testabilidad:** El contexto indica que no existen pruebas automatizadas ni análisis estático del código. Eso significa que cada vez que los desarrolladores hacen un cambio, no hay manera confiable de saber si rompieron algo que antes funcionaba. Esto lleva a que los errores lleguen hasta producción, lo que obliga a los agentes a arreglarlos manualmente y afecta la experiencia del cliente. Además, sin pruebas es difícil mantener y evolucionar el sistema con seguridad.

Escenario de calidad – Seguridad - Detección y bloqueo de accesos / operaciones no autorizadas

Fuente: Atacante externo o credenciales comprometidas.

Un atacante o alguien con credenciales robadas intenta acceder al sistema para abrir o modificar un CDT usando esas credenciales, posiblemente desde una ubicación o dispositivo inusual.

Estímulo: Intento de abrir o manipular un CDT usando credenciales robadas o solicitudes previamente anuladas.

El usuario (o atacante) enciende una sesión en la app o web y pulsa “Crear CDT” o “Modificar solicitud”, pero lo hace desde un dispositivo desconocido o IP geográficamente distinta a su comportamiento normal.

Artefacto: Servicio de autenticación, API de CDT, base de datos KYC (Know Your Costumer) y logs de auditoría.

El frontend envía la petición al servicio de autenticación y a la API de gestión de CDT. Posteriormente estos servicios consultan la base de datos KYC y generan eventos en los logs/auditoría.

Ambiente: Producción / uso real.

La situación ocurre en la versión en vivo de la app con usuarios reales, durante un horario normal con carga moderada. No es un pico extremo ni una caída de red masiva.

Respuesta: El sistema identifica la actividad sospechosa, bloquea la operación y pide verificación adicional; registra el evento y alerta al equipo de seguridad.

Se detecta que la sesión es anómala, la operación queda bloqueada, se muestra al usuario un mensaje claro (por ejemplo: “Actividad sospechosa: verifique por SMS/2FA”), se solicita un paso extra de verificación y el intento queda registrado en el log de auditoría; si no se verifica, la acción no se completa.

Medida de respuesta: ≥ 99.9% de intentos maliciosos detectados y bloqueados; tiempo medio de detección < 5 minutos; 100% de cuentas administrativas protegidas por 2FA.

Métrica de éxito:

- Detección y bloqueo efectivo en ≥ 99.9% de intentos maliciosos durante un periodo representativo (por ejemplo: 30 días).
- Tiempo medio de detección < 5 minutos.
- 100% de cuentas administrativas con 2FA activo.
- 0 vulnerabilidades críticas abiertas por despliegue (según SAST).

Estas métricas se revisan periódicamente (mensual/trimestral) para validar cumplimiento.

Escenario de calidad – Usabilidad – Registros reutilizables sin repetición de datos

Fuente: Usuario nuevo o existente que abre un CDT.

Un cliente quiere abrir un CDT desde la app o la web. Puede ser un usuario nuevo o uno que ya tiene datos en el sistema.

Estímulo: Inicia el proceso de apertura y presiona “Enviar” después de completar sus datos y subir documentos.

El usuario completa el formulario y pulsa “Enviar” para iniciar la verificación KYC (Know Your Costumer) y la creación de la solicitud de CDT.

Artefacto: Frontend (formularios), servicio KYC, repositorio/tabla de clientes y UI de estados.

El formulario envía los datos al servicio KYC, que consulta la base de datos de clientes para identificar duplicados y guarda la solicitud con su estado inicial.

Ambiente: App en condiciones normales de red.

La acción ocurre en uso diario, con concurrencia moderada y sin condiciones de pico extremo.

Respuesta: El sistema reutiliza datos existentes, guía el flujo y confirma la creación sin pedir repetir información innecesaria.

Si el usuario ya existe, el sistema no solicita de nuevo datos básicos; muestra pasos claros y el estado actual (por ejemplo: “Borrador → En validación → Aprobado”). Después de presionar “Enviar” el usuario ve una confirmación clara y la nueva solicitud aparece en su historial.

Medida de respuesta:

- Tasa de éxito end-to-end del registro ≥ 95%.
- Tiempo para completar registro (P95) ≤ 4 minutos.
- Tasa de abandono en registro < 5%.
- KYC duplicados en la base de datos < 1% (o reducción ≥ 90% respecto a estado previo).

Métrica de éxito:

- ≥ 95% de usuarios que inician el registro completan el proceso en el periodo de referencia (por ejemplo: 30 días).
- El 95º percentil del tiempo de completitud ≤ 4 minutos.
- Tasa de abandono durante el paso KYC < 5% por cohorte semanal.
- Porcentaje de clientes con registros duplicados < 1% en la base de datos (o reducción ≥ 90% respecto a línea base), medido mensualmente.

Escenario de calidad – Testabilidad – Cambios seguros sin romper el código

Fuente: Desarrollador que hace un cambio en el código.

Un desarrollador sube un cambio que modifica cómo se valida la información del cliente o cómo se crea una solicitud de CDT.

Estímulo: Pide fusionar (merge) ese cambio a la rama principal.

Al crear la solicitud de fusión, el sistema automático corre varias pruebas y chequeos antes de permitir que el cambio avance.

Artefacto: Repositorio de código y pipeline automático (pruebas y análisis).

El cambio pasa por pruebas rápidas (unitarias), pruebas más completas y un análisis de seguridad automático antes de poder integrarse.

Ambiente: Entorno de integración y staging (no se prueba en usuarios reales).

Las pruebas corren en un entorno controlado que imita al de producción, por lo que no se usan datos reales ni se afectan usuarios.

Respuesta: Si alguna prueba o el análisis de seguridad falla, el merge se bloquea y el cambio NO llega a producción; si todo pasa, el cambio se puede promocionar para pruebas finales y luego desplegar.

Sólo se permite avanzar cambios que no rompan funciones existentes y que no introduzcan problemas de seguridad.

Medida de respuesta:

- Cobertura mínima en código crítico (validaciones KYC/CDT) ≥ 80%.
- 0 vulnerabilidades críticas permitidas en cada PR; vulnerabilidades altas deben corregirse antes del merge.
- ≥ 95% de PRs con pipeline exitoso.
- Tiempo promedio para arreglar un bug crítico en staging < 24 horas.
- Tasa de rollback en producción ≤ 1% de despliegues al mes.

Métrica de éxito:

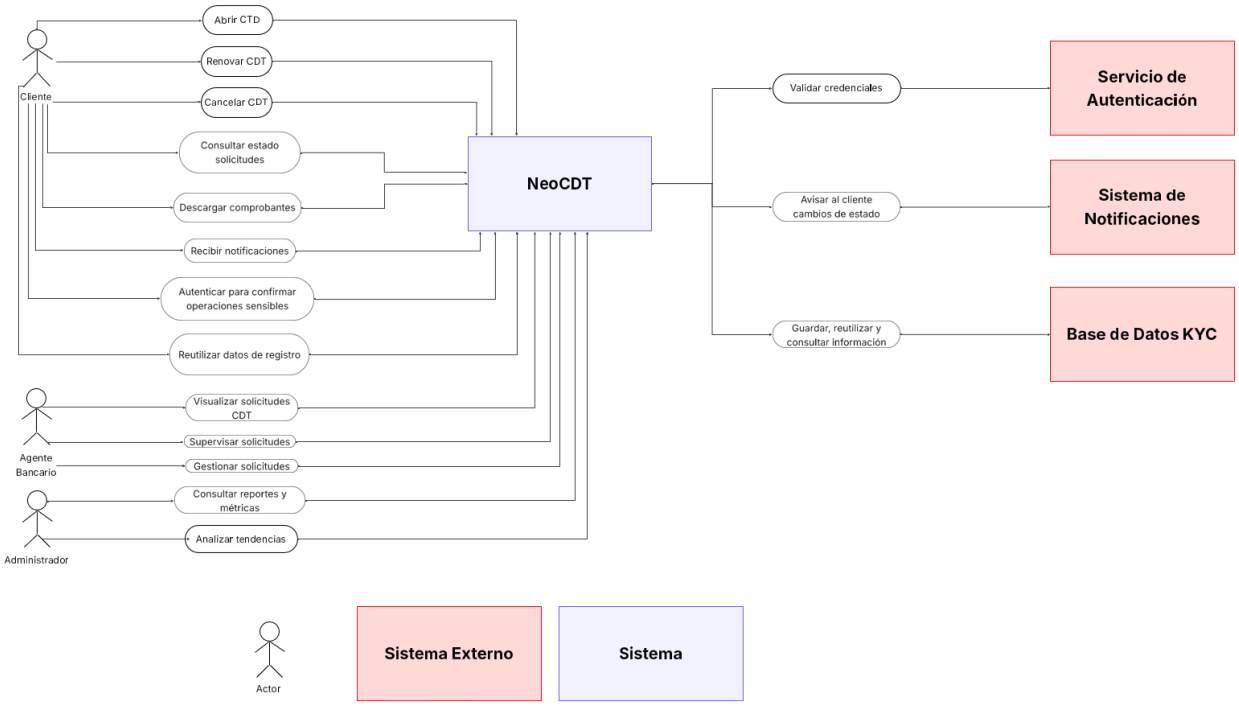
Que se cumplan las cinco medidas anteriores durante el periodo de referencia (por ejemplo: 30 – 90 días):

- cobertura ≥ 80%,
- 0 críticas en PRs,
- ≥ 95% builds verdes,
- MTTR < 24 h,
- rollbacks ≤ 1% mensual.

DISEÑO ARQUITECTONICO

Vistas Arquitectónicas

1. **Vista de Contexto**



La Vista de Contexto del sistema NeoCDT muestra cómo este se relaciona tanto con los actores humanos como con los sistemas externos necesarios para su funcionamiento.

En primer lugar, el Cliente es el actor principal, ya que interactúa con NeoCDT para abrir, renovar, cancelar y consultar Certificados de Depósito a Término (CDTs). Además, puede descargar comprobantes, recibir notificaciones y reutilizar sus datos previamente registrados para evitar reprocesos.

El Agente Bancario utiliza un panel centralizado que le permite visualizar, supervisar y gestionar las solicitudes de CDT, lo que reduce la carga de trabajo manual y mejora la eficiencia operativa. Por su parte, el Administrador consulta reportes y métricas del sistema, con el fin de analizar tendencias y tomar decisiones estratégicas basadas en datos.

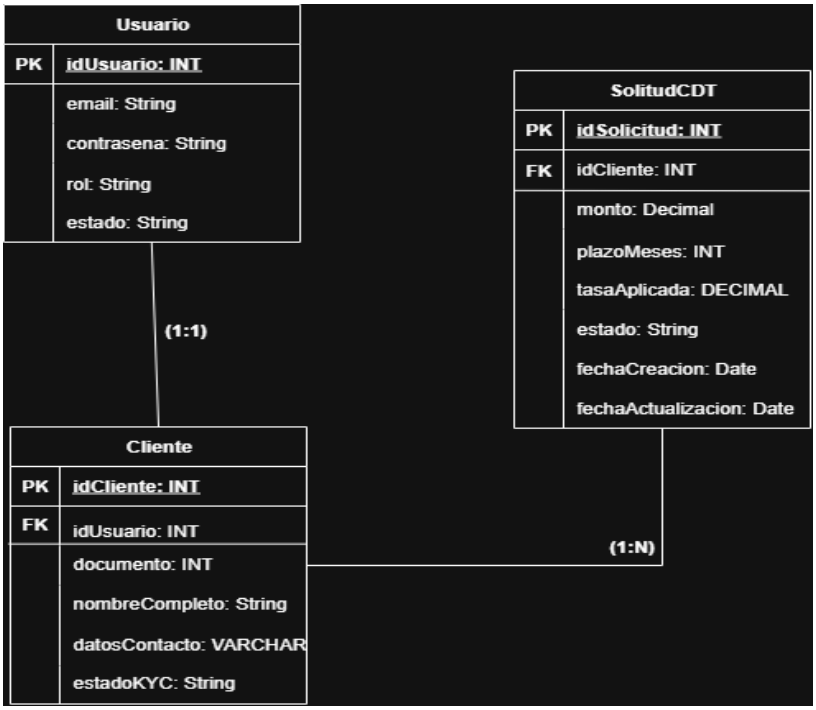
El sistema NeoCDT se apoya en tres componentes externos clave:

- El Servicio de Autenticación, encargado de validar credenciales y reforzar la seguridad de operaciones sensibles mediante autenticación multifactor.
- La Base de Datos KYC, donde se guarda, reutiliza y consulta la información de los clientes y de las solicitudes de CDT, garantizando trazabilidad y consistencia en los datos.

- El Sistema de Notificaciones, que se encarga de mantener informado al cliente mediante alertas sobre el estado de sus solicitudes (por correo, SMS o notificaciones push).

De esta forma, el diagrama refleja cómo NeoCDT centraliza la gestión de CDTs, a la vez que se conecta con usuarios y sistemas externos para ofrecer seguridad, transparencia y eficiencia en la operación.

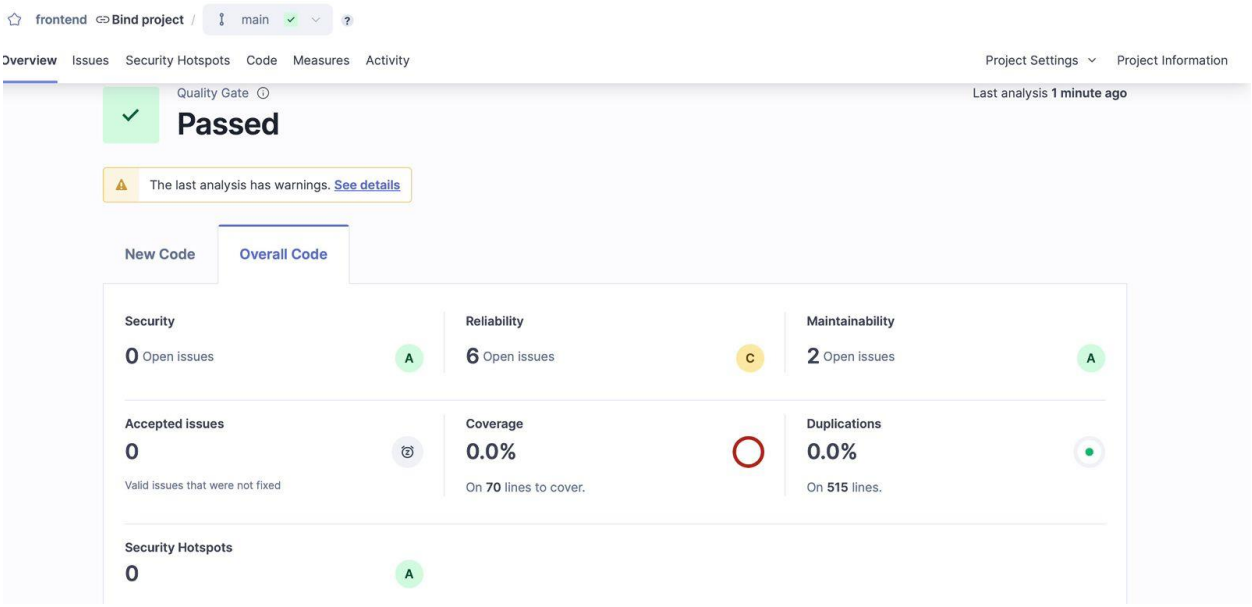
2. Vista de Información

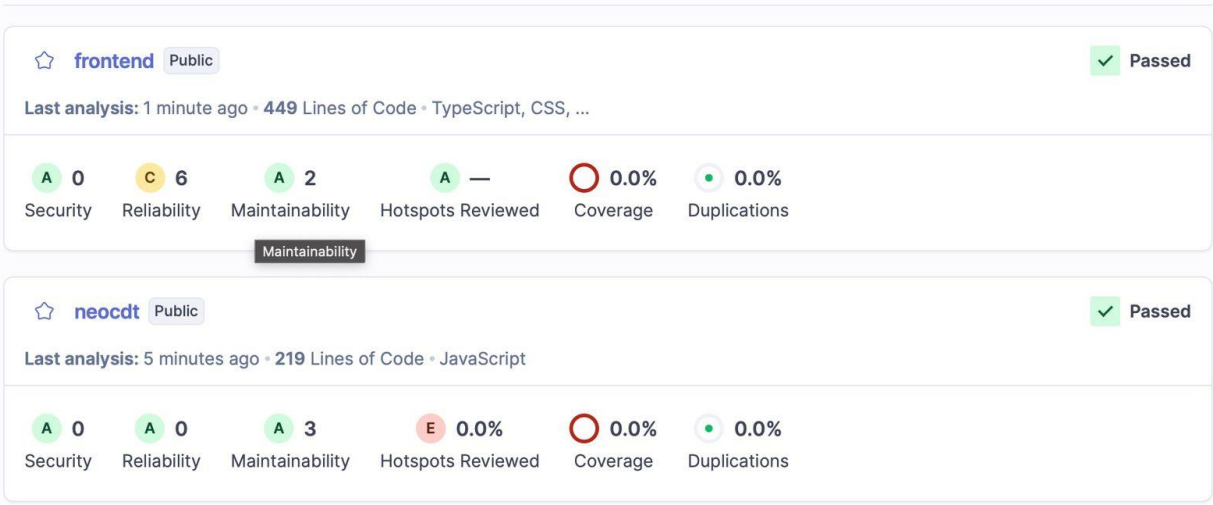


La Vista de Información del sistema NeoCDT se centra en tres entidades principales: Usuario, Cliente y SolicitudCDT. La entidad Usuario gestiona las credenciales de acceso y el rol dentro del sistema (cliente, agente o administrador). Cada Usuario se asocia de manera uno a uno con un Cliente, lo que significa que cada cliente registrado cuenta con un único perfil de acceso al sistema. La entidad Cliente contiene la información personal y regulatoria, incluyendo documento, nombre, datos de contacto y el estado KYC (*Know Your Customer*), que corresponde al proceso obligatorio en el sector financiero para verificar la identidad del cliente y cumplir con normativas de seguridad y prevención de fraude. A su vez, la entidad Cliente se relaciona de forma uno a muchos con SolicitudCDT, ya que un cliente puede generar varias solicitudes, pero cada solicitud pertenece únicamente a un cliente. La entidad SolicitudCDT registra la operación de apertura, renovación o cancelación de un certificado, con atributos como monto, plazo, tasa aplicada, estado, canal y fechas de creación y actualización. Estas relaciones aseguran consistencia y trazabilidad, ya que permiten vincular la autenticación de los usuarios con sus datos personales y con las solicitudes de productos financieros, garantizando un flujo centralizado y seguro en la gestión de CDTs.

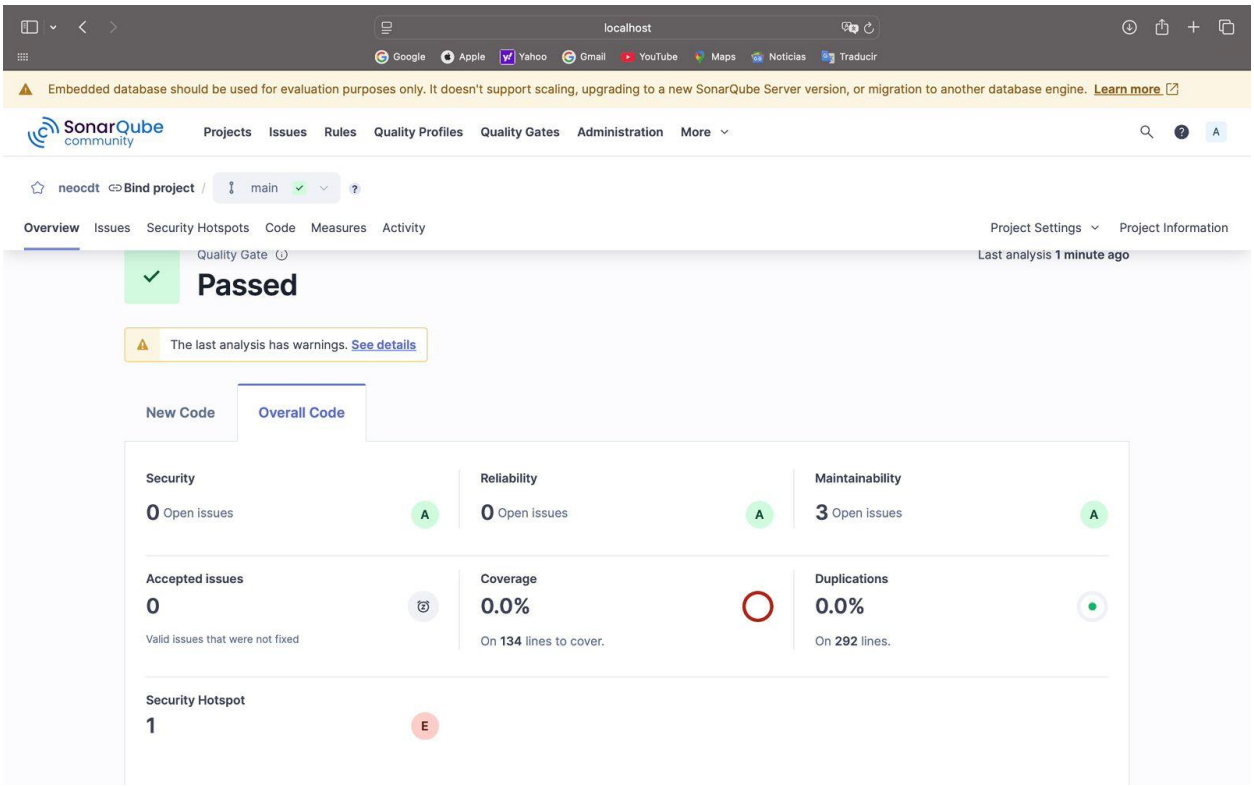
Pruebas SonarQube Segunda Entrega

Fronted



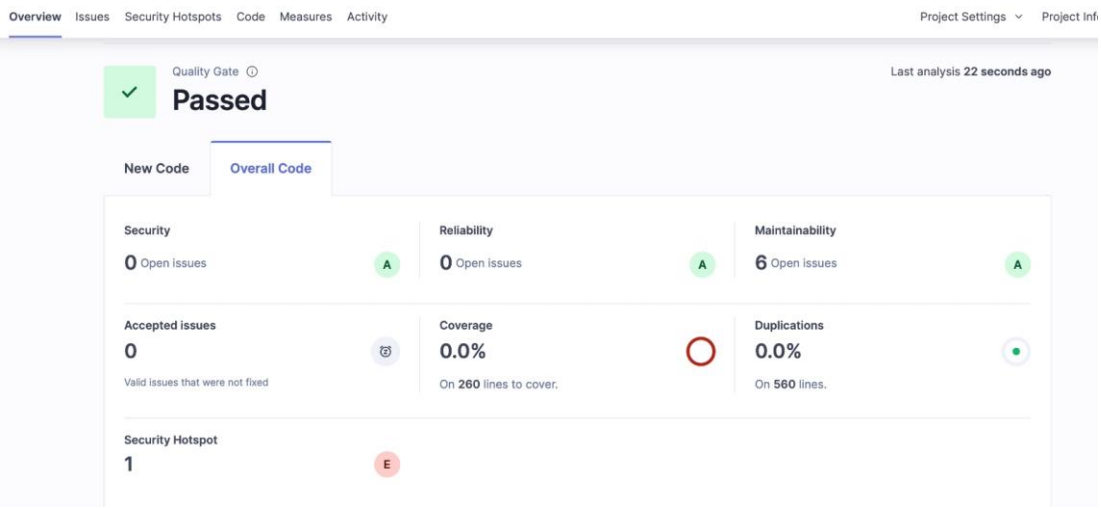


Backend

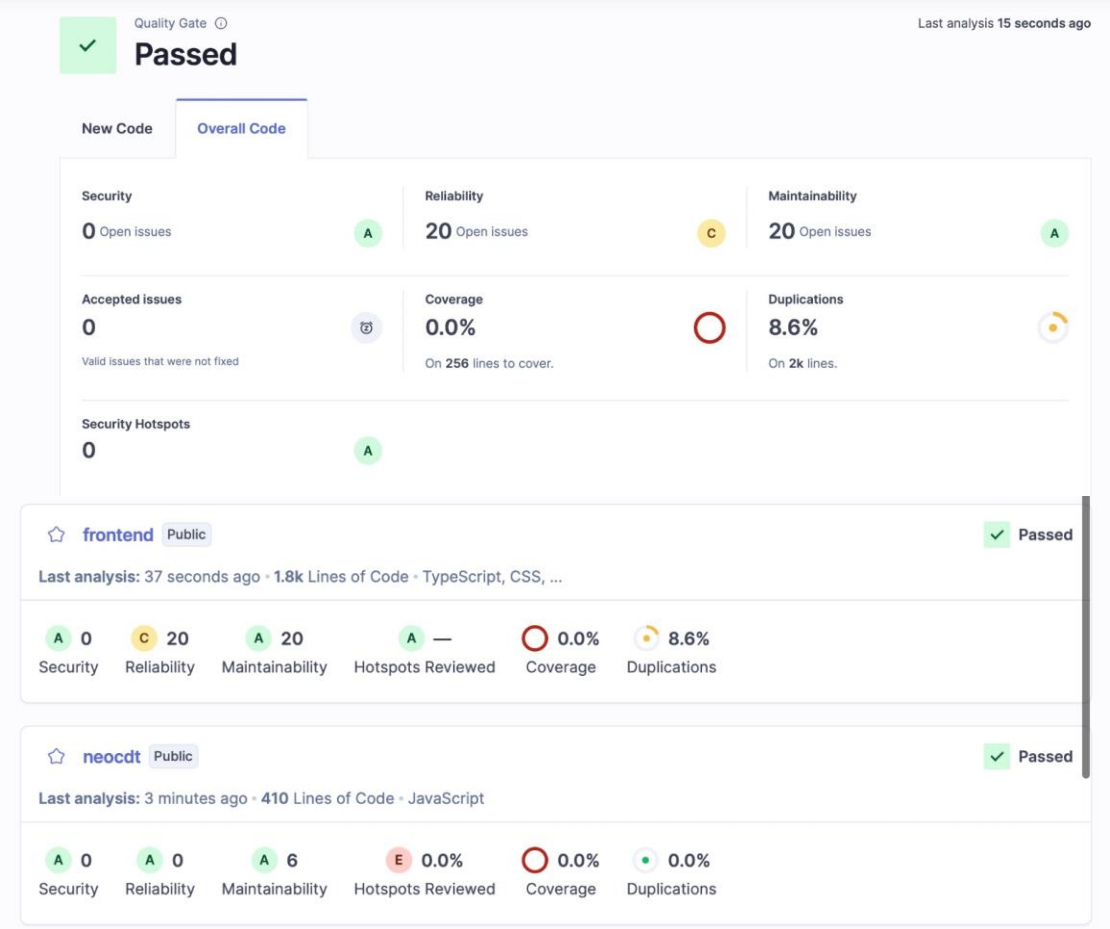


Pruebas SonarQube Primera Entrega

Backend


Overview
Issues
Security Hotspots
Code
Measures
Activity
Project Settings
Project Inf
Quality Gate
Passed
Last analysis 22 seconds ago
New Code
Overall Code
Security
0 Open issues
A
Reliability
0 Open issues
A
Maintainability
6 Open issues
A
Accepted issues
0
Valid issues that were not fixed
Coverage
0.0%
On 260 lines to cover.
Duplications
0.0%
On 560 lines.
Security Hotspot
1
E

Frontend


Quality Gate
Passed
Last analysis 15 seconds ago
New Code
Overall Code
Security
0 Open issues
A
Reliability
20 Open issues
C
Maintainability
20 Open issues
A
Accepted issues
0
Valid issues that were not fixed
Coverage
0.0%
On 256 lines to cover.
Duplications
8.6%
On 2k lines.
Security Hotspots
0
A
frontend
Public
Passed
Last analysis: 37 seconds ago • 1.8k Lines of Code • TypeScript, CSS, ...
A 0 Security
C 20 Reliability
A 20 Maintainability
A — Hotspots Reviewed
0.0% Coverage
8.6% Duplications
neocdt
Public
Passed
Last analysis: 3 minutes ago • 410 Lines of Code • JavaScript
A 0 Security
A 0 Reliability
A 6 Maintainability
E 0.0% Hotspots Reviewed
0.0% Coverage
0.0% Duplications