1️⃣ Objetivo central del sistema

Garantizar la **anonimización y separación de identidades** entre jueces y secretarias, asegurando:

- Asignación aleatoria de casos
- No revelación de identidades reales
- Trazabilidad (logs) sin romper anonimato
- Acceso controlado por tokens de un solo uso
- Integridad del dictamen enviado a la corte

2️⃣ Roles y responsabilidades (bien delimitados)

🏛️ Corte

Rol pasivo + verificador

- Mantiene **registro anonimizado** de jueces

- Recibe dictámenes
- Aprueba o rechaza dictámenes
- No conoce:
- Secretaria asignada
- Identidad real del juez
- Sí conoce:
- Identificador anónimo del juez
- Historial de dictámenes

Datos que maneja:

- judge_anon_id
- dictamen
- estado del dictamen
- timestamps

🛠️ Administrador

Rol de auditoría

- No interactúa con casos ni dictámenes
- Accede solo a:
- Logs del sistema
- Métricas agregadas

Puede ver:

- Número de jueces activos por día

- Cantidad de casos resueltos
- Accesos al sistema
- Tokens emitidos / usados / expirados (sin contenido)

No puede ver:

- Contenido de casos
- Identidad de jueces o secretarias

🗂️ Secretaria

Rol operativo

- Crea casos
- Administra estado del caso
- Envía casos a jueces de forma **aleatoria**
- Está ligada a un juez *lógico*, pero:
- No conoce su identidad
- No puede comunicarse directamente con él

Puede ver:

- Estado del caso (enviado, en dictamen, resuelto)
- ID del juez (anonimizado)

No puede ver:

- Correo real del juez
- Tokens
- Dictamen final (solo estado)

⚖️ Juez

Rol decisor

- Recibe tokens por correo
- Accede a casos solo mediante token
- Emite dictamen
- Envía dictamen a la corte

Puede ver:

- Casos asignados
- Su propio dictamen
- Estado de envío

No puede ver:

- Quién creó el caso
- Qué secretaria está asociada
- Otros jueces

3️⃣ División funcional del sistema

A. Gestión de identidades (IAM)

- Usuarios con IDs internos
- Separación entre:
- Identidad real
- Identidad lógica/anonimizada
- Mapping protegido (solo sistema)

Ejemplo:

UserID → Role → AnonID

B. Gestión de casos

- Crear caso
- Asignar juez aleatoriamente
- Cambios de estado:
- Creado
- Asignado
- En dictamen
- Enviado a corte
- Aprobado / Rechazado

C. Sistema de tokens (núcleo de seguridad)

Aquí está lo más importante 👇

Token por caso

- Único
- Ligado a:
- juez
- caso
- De un solo uso
- Estado:
- activo
- usado
- expirado

Flujo:

- Secretaria crea caso
- Sistema asigna juez random
- Sistema genera token
- Token se envía por correo al juez
- Juez accede al caso usando token
- Token se invalida al enviar dictamen

✔ El token **no caduca por tiempo**, sino por **evento** (envío de dictamen)

D. Acceso del juez (sin sesiones

temporales)

Tu decisión es correcta 👍

- El juez tiene sesión normal
- Los casos aparecen en una “cola”
- Para abrir un caso:
- Debe ingresar el token correspondiente
- El token:
- Se valida
- Se marca como usado
- Se asocia al dictamen

Esto evita:

- Accesos accidentales
- Reutilización
- Acceso a casos no autorizados

E. Envío y validación del dictamen

- Dictamen firmado digitalmente (ideal)
- Hash del dictamen almacenado
- Enviado a la corte
- Corte valida:

- Integridad
- Autor anónimo
- Estado del caso

4️⃣ Seguridad y anonimización (por capas)

🔐 Anonimización

- IDs aleatorios (UUID)
- Separar tablas:
- Identidad real
- Identidad lógica
- Cifrado en reposo

🧾 Logs

- Logs inmutables
- Sin datos sensibles
- Solo IDs anonimizados

📧 Correo

- Solo canal de entrega del token
- Token no revela:
- Caso

- Secretaria
- Idealmente token + enlace