11. Gestión de datos en red

La gestión de datos en red del Sistema de Gestión de Reclamos de Agua Potable se centra en asegurar el intercambio eficiente, seguro y consistente de la información entre la capa móvil, la capa web y el servidor central de SEDAM. Para ello se implementan las siguientes prácticas:

11.1. Transmisión de datos mediante API REST

Toda la información (usuarios, reclamos, estados, evidencias, notificaciones) se gestiona mediante servicios REST, los cuales permiten intercambiar datos en formato JSON de forma estructurada y controlada entre cliente y servidor.

11.2. Sincronización en tiempo real

Los reclamos, cambios de estado, evidencias y notificaciones se actualizan en tiempo real a través de peticiones HTTP seguras, evitando inconsistencias entre web y móvil.
El sistema garantiza que los datos mostrados al ciudadano y a los operadores estén siempre actualizados.

11.3. Sincronización en tiempo real

Para evitar conflictos cuando varios operadores gestionan un mismo reclamo, el servidor aplica:

- Validaciones de estado previo
- Transacciones ACID en la base de datos
- Bloqueos lógicos en operaciones críticas

Esto evita duplicidad de registros o actualizaciones incorrectas**.**

11.4. Sincronización en tiempo real

La base de datos se encuentra normalizada (3FN), lo que garantiza integridad referencial entre:

- usuario–ciudadano–operador
- reclamo–estado–historial
- reclamo–evidencias
- reclamo–notificaciones
- reportes–formatos oficiales

Esto permite que los datos viajen en red sin duplicación ni pérdida de integridad.

11.5. Sincronización en tiempo real

Antes de que los datos se envíen por la red:

- el cliente (web/móvil) valida formato y obligatoriedad
- el servidor valida reglas de negocio

Esto evita errores y reduce el tráfico innecesario en la red.

12. Seguridad en red y móviles

La seguridad en red y móviles se aplica para proteger la información transmitida, los dispositivos que se conectan al sistema y la infraestructura de SEDAM.

12.1. Cifrado de comunicación

Toda interacción entre aplicación móvil, web y servidor se realiza usando:

- HTTPS con TLS 1.2 o superior

Esto evita intercepciones o manipulaciones de datos sensibles.

12.2. Seguridad de acceso para usuarios móviles

Los dispositivos móviles utilizan:

- almacenamiento seguro para el token de sesión
-
- expiración programada del token
-
- bloqueo de sesión ante intentos fallidos

Así se evita que terceros accedan si el dispositivo se pierde o es robado.

12.3. Protección contra ataques de red

Para evitar conflictos cuando varios operadores gestionan un mismo reclamo, el servidor aplica:

- Validaciones de estado previo
- Transacciones ACID en la base de datos
- Bloqueos lógicos en operaciones críticas

Esto evita duplicidad de registros o actualizaciones incorrectas.

12.4. Subida segura de evidencias

Las evidencias enviadas desde el móvil (fotos, PDF, videos):

- viajan cifradas
- son filtradas por tipo y tamaño
- pasan por un antivirus del servidor
- se almacenan en rutas seguras

12.5. Integridad de la aplicación móvil

Para evitar aplicaciones falsificadas o manipuladas:

- verificación de firma digital
- bloqueo de apps modificadas
- detección básica de root/jailbreak

12.6. Seguridad en servidor y red interna

El backend y la base de datos están aislados en una red interna privada, evitando accesos directos desde internet y reduciendo riesgos de intrusión.

13. Justificación técnica

La implementación del Sistema de Gestión de Reclamos de Agua Potable se basa en un conjunto de decisiones técnicas que garantizan la eficiencia, seguridad, compatibilidad y escalabilidad del sistema. Cada elemento del diseño —desde la comunicación entre la interfaz y el servidor hasta la gestión de datos en red y la seguridad en entornos móviles— ha sido seleccionado para asegurar un funcionamiento confiable y adaptado al contexto institucional de SEDAM.

13.1. Justificación de la arquitectura técnica

El uso de una arquitectura en capas (N-Tier) es apropiado debido a que separa claramente la presentación, la lógica de negocio y el acceso a datos, lo cual facilita el mantenimiento y reduce el riesgo de errores entre componentes. Esta estructura permite que la interfaz web funcione de manera independiente del motor de base de datos y que la lógica de negocio pueda modificarse sin afectar la visualización o la infraestructura.
Además, esta arquitectura se ajusta al tamaño y a la naturaleza centralizada de SEDAM, evitando la complejidad innecesaria de arquitecturas distribuidas como microservicios.

13.2. Justificación del modelo de comunicación

La elección de HTTP/HTTPS como protocolo principal responde a su compatibilidad universal con cualquier navegador o dispositivo, permitiendo que el sistema funcione sin instalaciones adicionales. El uso de HTTPS garantiza comunicaciones cifradas, especialmente relevantes cuando los ciudadanos transmiten datos sensibles o cargan evidencias desde redes móviles o públicas.
El formato JSON complementa esta elección, ya que es ligero, eficiente y procesado nativamente por JavaScript, optimizando el rendimiento y reduciendo el consumo de datos de los usuarios móviles.

13.3. Justificación del diseño web y su estructura

El enfoque de diseño simple y orientado a la claridad facilita el acceso de todo tipo de usuarios, incluyendo ciudadanos con poca experiencia tecnológica. Formularios ordenados, retroalimentación inmediata y navegación directa reducen las posibilidades de error y hacen que el registro de reclamos y la consulta de estados sean procesos rápidos y comprensibles.
La estructura modular del sistema web se alinea con las buenas prácticas de diseño responsivo, asegurando funcionamiento en computadoras y dispositivos móviles sin desarrollar aplicaciones nativas adicionales.

13.4. Justificación de la tolerancia a fallos.

El sistema incorpora mecanismos para mantener su operatividad incluso frente a condiciones adversas, como caídas temporales del servidor o baja estabilidad de red.
Medidas como reintentos controlados, mensajes claros al usuario, transacciones ACID y bloqueos lógicos evitan pérdidas de información o inconsistencias en los reclamos.
Esto es crucial porque el sistema maneja datos oficiales y evidencias, cuyos registros deben ser precisos y verificables.

13.5. Justificación de la gestión de datos en red

La decisión de utilizar servicios REST permite un intercambio de datos estructurado, seguro y estándar entre la interfaz web, el servidor y la base de datos.
El control de concurrencia impide que varios operadores generen inconsistencias al gestionar un mismo reclamo.
Además, la normalización de la base de datos y su uso en red aseguran integridad referencial y un manejo eficiente de la información institucional, facilitando auditorías, reportes y trazabilidad completa del proceso.

13.7. Justificación de las medidas de seguridad en red y móviles

La seguridad se aborda desde varios niveles:

- cifrado TLS para proteger toda la comunicación,
- tokens de sesión seguros en móviles,
- controles de roles para restringir funciones entre ciudadanos y operadores,
- firewalls y validación interna para evitar ataques externos,
- verificación de evidencias para prevenir archivos maliciosos.

Estas medidas son indispensables porque el sistema maneja datos personales, reportes institucionales y material multimedia que debe protegerse contra accesos no autorizados y modificaciones indebidas. La protección de dispositivos móviles y la integridad de la aplicación fortalecen el uso seguro en campo por parte de operadores y ciudadanos.

13.8. Justificación del uso de patrones de diseño

La elección de patrones como DAO, Observer y Fachada permite mantener un sistema modular, fácil de expandir y técnicamente sólido:

- DAO separa la lógica de negocio del acceso a datos.
- Observer automatiza notificaciones sin acoplar módulos.
- Fachada simplifica la coordinación de procesos complejos como el registro de reclamos.

Estos patrones reducen errores, facilitan la reutilización del código y garantizan un funcionamiento claro y estandarizado en todos los módulos.