Ingeniería de Software II

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

TP2

Alerta y Vigliancia de Yacimientos Semi-Automatico
AVYSA
2 de julio de 2017

Integrante	LU	Correo electrónico
Christian Cuneo	755/13	chriscuneo93@gmail.com
Federico Beuter	827/13	federicobeuter@gmail.com
Mauro Cherubini	835/13	cheru.mf@gmail.com
Mario Ezequiel Ginsberg	145/14	ezequielginsberg@gmail.com
Martin Baigorria	575/14	martinbaigorria@gmail.com

Reservado para la cátedra

Instancia	Docente	Nota
Primera entrega		
Segunda entrega		

Índice

1. Casos de uso

1.1. Diagrama

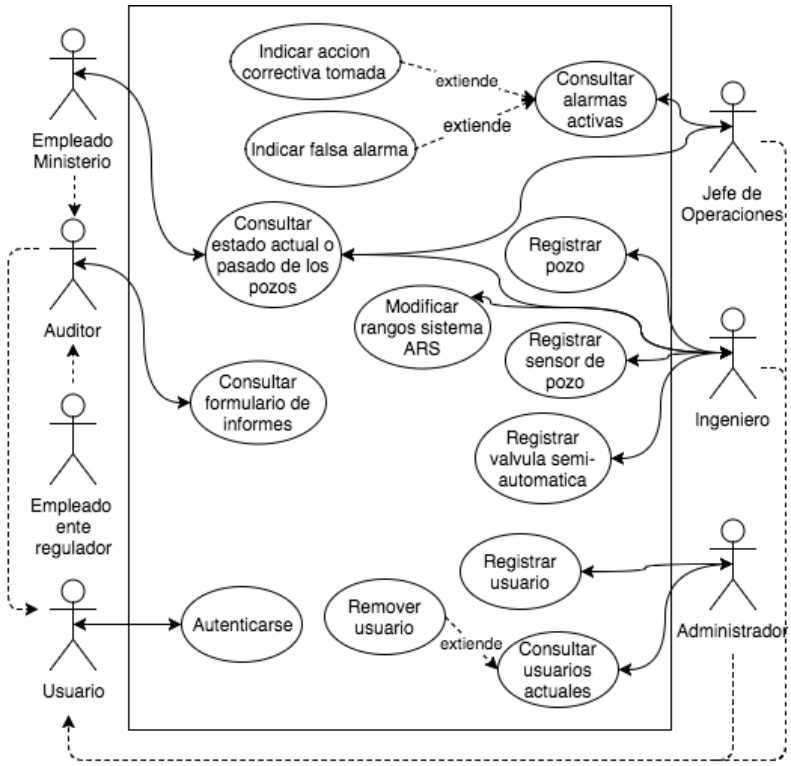

Figura 1: Diagrama de casos de uso

1.2. Descripción

1. **Autenticándose**: La primera acción que tiene que realizar cualquier usuario, no importe su perfil, para poder seguir interactuando con el sistema con los permisos que tenga su perfil.
2. **Registrando usuario**: La forma que tiene el administrador de ingresar un nuevo usuario al sistema, indicando el perfil que va a utilizar.
3. **Removiendo usuario**: El administrador le saca el acceso al sistema a un usuario en particular.
4. **Consultando usuarios actuales**: El administrador lista los usuarios actuales.
5. **Registrando pozo**: De esta forma el ingeniero hace que el sistema considere un nuevo pozo en su procesamiento y lo agregue al simulador de simoil entre otras cosas.
6. **Registrando sensor de pozo**: El ingeniero registra un nuevo sensor indicando el pozo al que pertenece para que el sistema sepa a que pozo pertenece.
7. **Registrando válvula semiautomática**: El ingeniero registra una nueva válvula semiautomática indicando el pozo al que pertenece y su función.
8. **Modificando rangos de sistema ARS**: Se modifican los rangos de limpieza de datos.
9. **Consultando estado actual o pasado de los pozos**: Para consultar una historia de los valores de los sensores, posiciones de las válvulas y estados de alerta para cada pozo.
10. **Consultando formulario de informes**: Se listan los informes detallados de eventos detectados por el sistema.
11. **Consultando alarmas activas**: De esta forma el jefe de operaciones tiene acceso a las alarmas activas.

12. **Indicando falsa alarma**: El jefe de operaciones cierra una alarma indicando que fue falsa alarma.
13. **Indicando acción correctiva tomada**: El jefe de operaciones cierra una alarma indicando la acción correctiva tomada.

1.3. Especificacion

En esta sección identificaremos los tres casos de uso principales y los especificaremos en detalle utilizando la tabla de curso normal/alternativo.

Caso de Uso: Registrar válvula semiautomática

Curso Normal	Curso Alternativo
1. El ingeniero selecciona la opción de ingresar una válvula	
2. El sistema carga el listado de pozos actuales y sus válvulas	
3. El ingeniero selecciona un pozo al que corresponde la válvula	
4. El sistema carga el listado de tipos de válvula	
5. El ingeniero selecciona que tipo de válvula a ingresar	5.1. La válvula del tipo seleccionado ya fue ingresada para ese pozo. Vuelve a 5.
6. El ingeniero confirma selección	
7. El sistema persiste la válvula	
8. El sistema informa éxito de operación	
9. Fin del caso	

Caso de Uso: Indicar acción correctiva tomada

Curso Normal	Curso Alternativo
1. El jefe de operaciones selecciona la opción de indicar acción correctiva para la alarma seleccionada en la lista de alarmas activas	
2. El sistema carga en detalle la alarma seleccionada	
3. El jefe de operaciones indica de forma detallada la acción tomada	
4. El jefe de operaciones confirma la operación	4.1 Descripción es muy corta, vuelve a 3
5. El sistema persiste la acción	
6. El sistema completa el informe de la alarma	
7. Fin del caso	

Caso de Uso: Consultar estado actual o pasado de los pozos

Curso Normal	Curso Alternativo
1. El usuario selecciona la opción de listar los pozos	
2. El sistema lista los pozos	
3. El usuario selecciona el pozo a consultar	
4. El sistema encuentra los registros de estados de válvulas para ese pozo	
5. El sistema encuentra los registros de estados de sensores para ese pozo	
6. El sistema encuentra los registros de alertas para ese pozo	
7. El sistema muestra de forma detallada el historial y el estado actual de este pozo	
8. Fin del caso	

2. Atributos de calidad

Luego del Quality Attribute Workshop (QAW), la priorización de los atributos de calidad fue la siguiente:

- Performance
- Disponibilidad
- Seguridad
- Usabilidad

Para cada tipo de atributo de calidad definimos distintos escenarios de acuerdo a lo relevado.

2.0.1. Performance

1)

- Descripción: La búsqueda de eventos en el sistema debe tardar a lo sumo medio segundo.
- Fuente: Auditor.
- Estímulo: Escribe en el buscador el evento a buscar y aprieta el botón Buscar.
- Artefacto: Sistema de Informes de Eventos.
- Entorno: Normal.
- Respuesta: Se obtienen los datos del evento buscado. Si la búsqueda es idéntica a otra realizada hace menos de 1 hora, la respuesta llegará más rápido.
- Medición: El sistema responderá la búsqueda en menos de 100 ms en el caso de una búsqueda repetida recientemente, y en menos de 500 ms en cualquier otro caso.

2)

- Descripción: La limpieza de datos deberá remover aproximadamente el 80 % de los picos no realistas del conjunto de datos.
- Fuente: Interna.
- Estímulo: Llegan nuevos datos a ser limpiados de datos no realistas.
- Artefacto: Sistema de Procesamiento de Mediciones.
- Entorno: Normal.
- Respuesta: El sistema realiza la limpieza de datos correctamente.
- Medición: Aproximadamente el 80 % de los picos fuera de los límites superior e inferior fueron eliminados del conjunto de datos.

3)

- Descripción: La detección de anomalías no debe tardar más de 5 minutos.
- Fuente: Interna.
- Estímulo: Llegan nuevos datos anómalos a ser analizados.
- Artefacto: Detector de Anomalías.
- Entorno: Normal.
- Respuesta: Se detectan las anomalías y se da aviso al Gestor de Anomalías.
- Medición: Las anomalías son detectadas en menos de 5 minutos.

4)

- Descripción: Ante un pronóstico catastrófico, la alarma debe ser envíada inmediatamente.
- Fuente: Interna.
- Estímulo: Evento catastrófico detectado por el módulo Detector de Anomalías.
- Artefacto: Gestor de Anomalías.
- Entorno: Normal.
- Respuesta: Envío inmediato de SMS al Jefe de Operaciones del yacimiento.
- Medición: El SMS se envía en menos de 50 ms.

2.0.2. Disponibilidad

1)

- Descripción: El sistema de procesamiento de mediciones debe estar en funcionamiento todo el tiempo para garantizar la mayor efectividad de detección de catástrofes.
- Fuente: Interna.
- Estímulo: Llegan datos a ser analizados.
- Artefacto: Sistema de Procesamiento de Mediciones.
- Entorno: Degradado.
- Respuesta: El sistema envía los datos a otra instancia de procesamiento de mediciones.
- Medición: En el 99.99999999 % de los casos los datos se procesaron correctamente.

2)

- Descripción: El formulario de eventos debe estar disponible en todo momento para el Ministerio y para el Ente Regulador de Seguridad Medio Ambiental.
- Fuente: Externa.
- Estímulo: Petición para visualizar el formulario de eventos.
- Artefacto: Sistema de Informes de Eventos.
- Entorno: Degradado.
- Respuesta: El balanceador de carga asigna otro sistema de informes de eventos para realizar la petición.
- Medición: En el 99.99999999 % de los casos los datos se visualizaron correctamente.

3)

- Descripción: El sistema en su totalidad debe ser tolerante a fallas.
- Fuente: Interna.
- Estímulo: Un módulo del sistema deja de funcionar.
- Artefacto: Sistema.
- Entorno: Normal.
- Respuesta: El sistema omite el módulo degradado.
- Medición: El sistema sigue en funcionamiento.

4)

- Descripción: El servicio de envío de SMS debe estar siempre en funcionamiento.
- Fuente: Externa.
- Estímulo: Se recibe un mensaje de error de envío de SMS.
- Artefacto: Gestor de Anomalías.
- Entorno: Normal.
- Respuesta: Se envía nuevamente el SMS por otro canal de envío de SMS.
- Medición: Se recibe una confirmación de envío del mensaje en menos de 1 minuto.

5)

- Descripción: En caso de siniestro, todos los registros deben mantenerse accesibles.
- Fuente: Interna.
- Estímulo: Se desea acceder a un registro.
- Artefacto: Gestor de Anomalías.
- Entorno: Degradado.
- Respuesta: El sistema redirige la petición al Gestor de Backups.
- Medición: Los datos son obtenidos en el 99.99999999 % de las veces.

2.0.3. Seguridad

1)

- Descripción: La autenticación de los usuarios debe ser segura.
- Fuente: Agente Externo.
- Estímulo: Un agente externo intenta interceptar los datos de un usuario cuando son enviados al sistema para el logueo en el mismo.
- Artefacto: Sistema de Usuarios.
- Entorno: Normal.
- Respuesta: Los datos se envían de forma segura.
- Medición: Debido al método de seguridad usado para enviar los datos, en menos del 0.00000001 % de los casos el agente externo logra descifrar los datos en menos de 1 semana.

2)

- Descripción: Los datos de los servicios externos se deben recibir de forma segura.
- Fuente: Agente Externo.
- Estímulo: Un agente externo intenta interceptar los datos de los servicios externos cuando son enviados al sistema para el procesamiento de los mismos.
- Artefacto: Controlador de válvula semiautomática.
- Entorno: Normal.
- Respuesta: Los datos son recibidos de forma segura.
- Medición: Debido al método de seguridad usado para enviar los datos, en menos del 0.00000001 % de los casos el agente externo logra descifrar los datos en menos de 1 semana.

3)

- Descripción: Un determinado perfil de usuario sólo puede ejecutar las acciones permitidas por dicho perfil.
- Fuente: Usuario.
- Estímulo: Intenta realizar una acción para la cual no está autorizado su perfil.
- Artefacto: Sistema.
- Entorno: Normal.
- Respuesta: El sistema invalida la acción y muestra un mensaje de error indicando la incompatibilidad de la acción con el perfil del usuario.
- Medición: En el 99.99999999 % de las veces la acción no va a ser permitida por el sistema.

2.0.4. Usabilidad

1)

- Descripción: El sistema debe ser fácil de aprender a usar y agradable a la vista.
- Fuente: Usuario.
- Estímulo: Interactúa con el sistema.
- Artefacto: Interfaz de Usuario.
- Entorno: Ejecución.
- Respuesta: Responde con mensajes claros y precisos, y muestra de forma simple y elegante las distintas acciones posibles dentro del sistema.
- Medición: Cualquier usuario debe poder aprender a usar el sistema en menos de 10 minutos.

2.0.5. Modificabilidad

1)

- Descripción: El sistema debe poder permitir el agregado de nuevos procesos para trabajar con los datos almacenados sin mucha dificultad.
- Fuente: Desarrollador.
- Estímulo: Quiere agregar un nuevo proceso.
- Artefacto: Sistema.
- Entorno: En diseño.
- Respuesta: Se realizan los cambios sin afectar las otras funcionalidades.
- Medición: Se agregó el nuevo proceso modificando sólo 2 módulos.

3. Arquitectura

3.1. Diagrama general

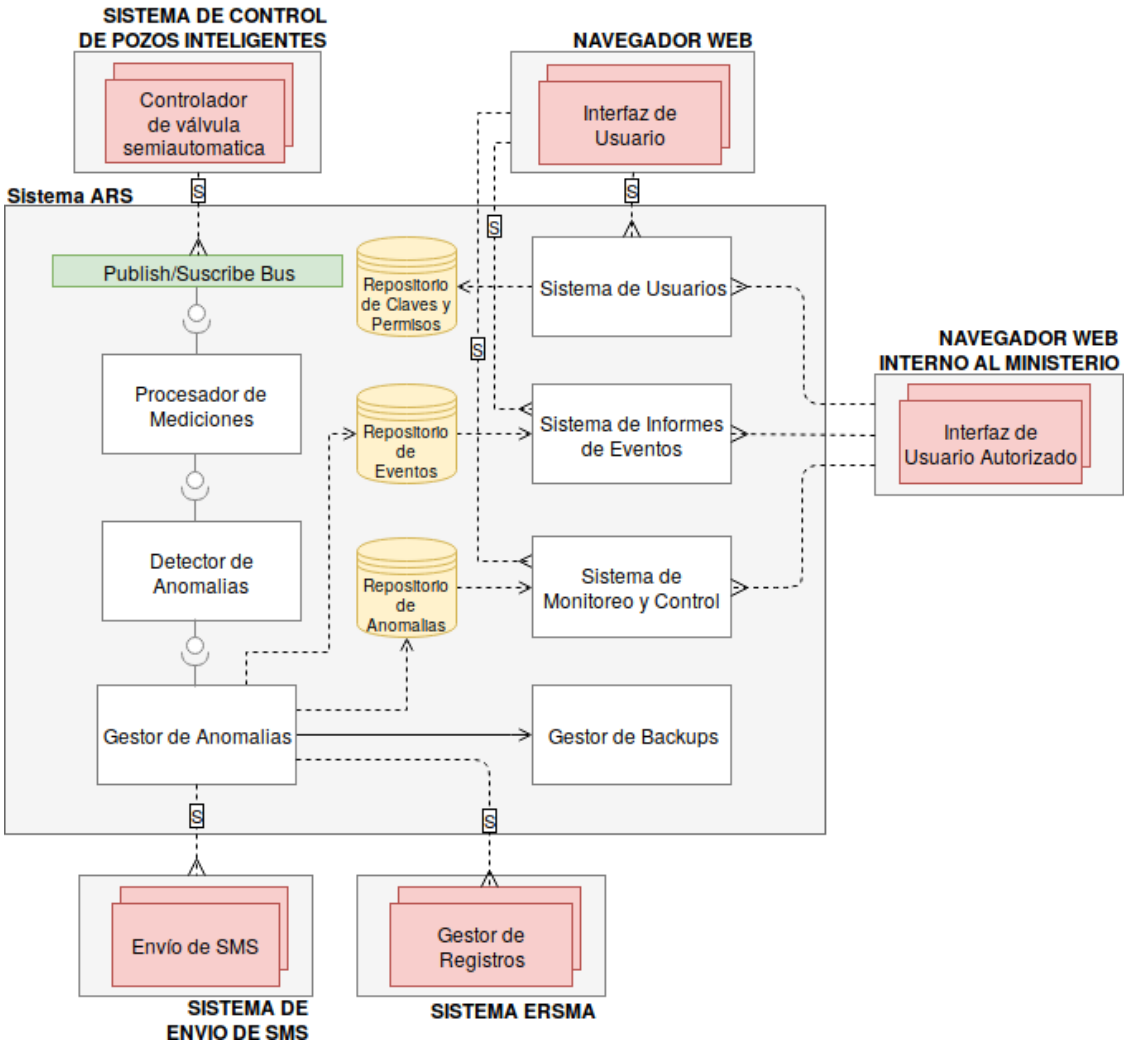

Figura 2: Diagrama general de la arquitectura del sistema ARS de supervisión automática de yacimientos.

La arquitectura del Sistema ARS busca procesar los datos de alta frecuencia que son producidos por los diferentes controladores de válvula semiautomática del Sistema de Control de Pozos Inteligentes (SCPO). Cada controlador publica las mediciones de la válvula en un Publish/Suscribe Bus al que esta suscripto el componente de Procesamiento de Mediciones. El Procesador de Mediciones (sección 3.2) básicamente se ocupa de transformar los datos de forma tal que puedan ser consumidos por el Detector de Anomalías.

El Detector de Anomalías (sección 3.3) identifica las diferentes anomalías en las mediciones, que son consumidas por el Gestor de Anomalías (sección 3.4). Este componente notifica por SMS al Jefe de Operaciones del yacimiento de que se ha producido una anomalía, y a su vez guarda diferentes registros en los repositorios de Eventos y Anomalías para que luego puedan ser accedidos de forma externa. El componente también se comunica con un Gestor de Backups para garantizar la integridad de los datos ante casos de perdida o siniestros. Para cumplir con las normas internacionales, toda anomalía también es reportada a los organismos certificadores de calidad como el Ente Regulador de Seguridad Medio Ambiental (ERSMA). Para garantizar la confidencialidad de los datos, toda comunicación con un sistema externo es cifrada usando algoritmos simétricos y de clave publica/privada.

Todo usuario que queda acceder al Sistema de Informes de Eventos y al Sistema de Control y Monitoreo se debe autenticar por medio del Sistema de Usuarios. De esta forma los empleados del Ministerio y el Ente Regulador pueden acceder a los datos en todo momento.

3.2. Procesamiento de mediciones

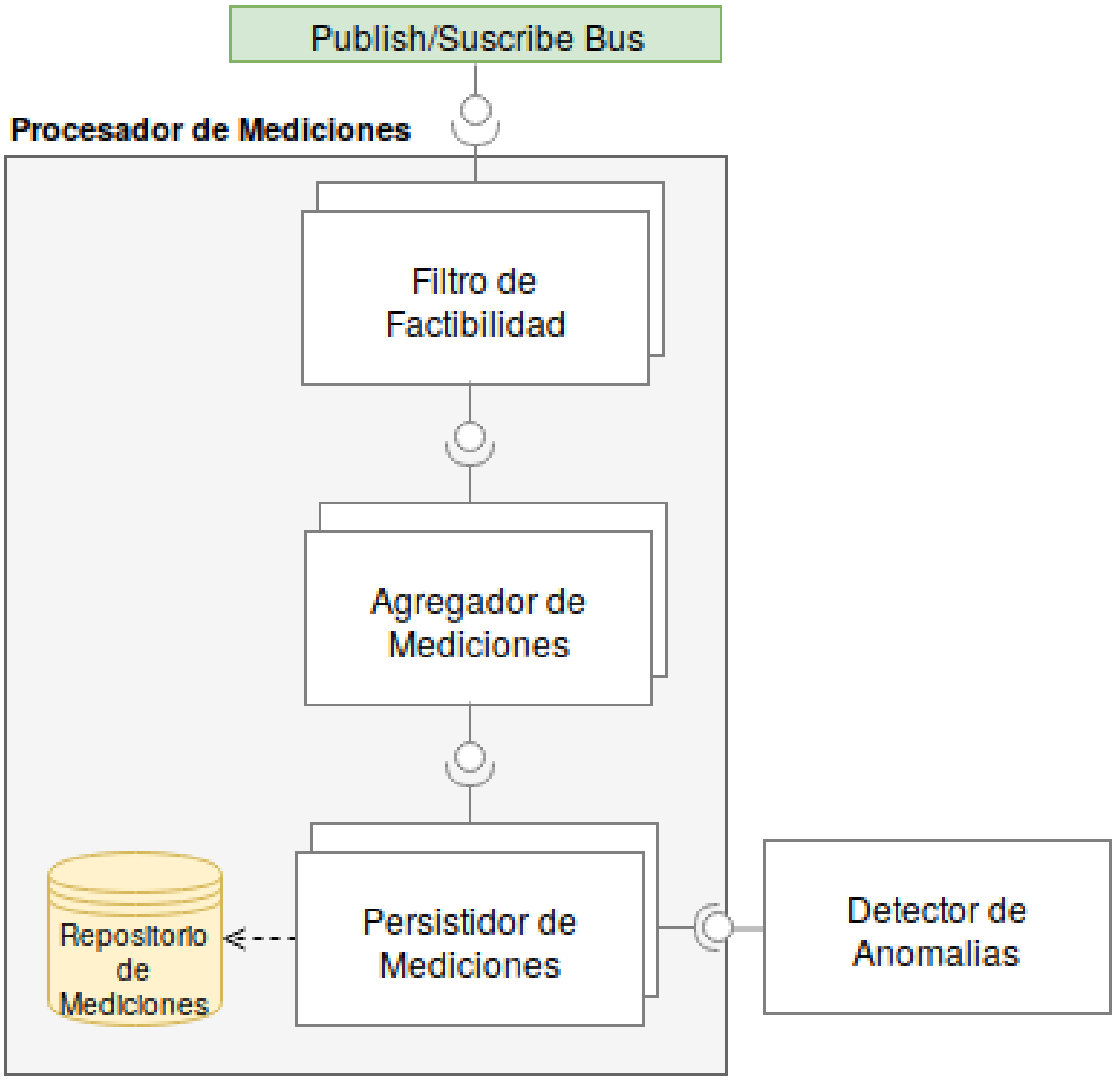

Figura 3: Diagrama de arquitectura de procesamiento de mediciones.

El Procesador de Mediciones consume datos de los diferentes controladores de válvula semiautomática de cada pozo a través de un Publish/Suscribe bus y una cola. Dada la alta frecuencia de los datos, no es factible ni practico guardarlos todos en una primera instancia antes de comenzar su procesamiento. Para reducir la cantidad de datos, primero se corre un Filtro de Factibilidad para remover los datos que no son realistas. Este filtro logra remover el 80 % de los datos espurios. Luego, los datos son agregados por el Agregador de Mediciones, el cual transforma los datos de alta frecuencia en datos en intervalos manejables de 15 minutos. Estos datos son luego consumidos por un Persistidor de Mediciones, que guarda los datos procesados y de menor dimensionalidad en un Repositorio de Mediciones. Estos datos también son enviados por medio de una cola al Detector de Anomalías.

Un dato que consideramos interesante explorar es la alta frecuencia de los datos. En caso de una caída del sistema, guardar los datos en un Repositorio luego del proceso de filtrado puede no ser relevante, dado que al momento en el que el sistema logra recuperarse rápidamente de una caída, datos muy similares van a ser incorporados desde los controladores de pozo inmediatamente, detectando posteriormente las mismas anomalías que hubiesen sido detectadas en caso de que el sistema hubiese funcionado correctamente.

3.3. Detector de anomalías

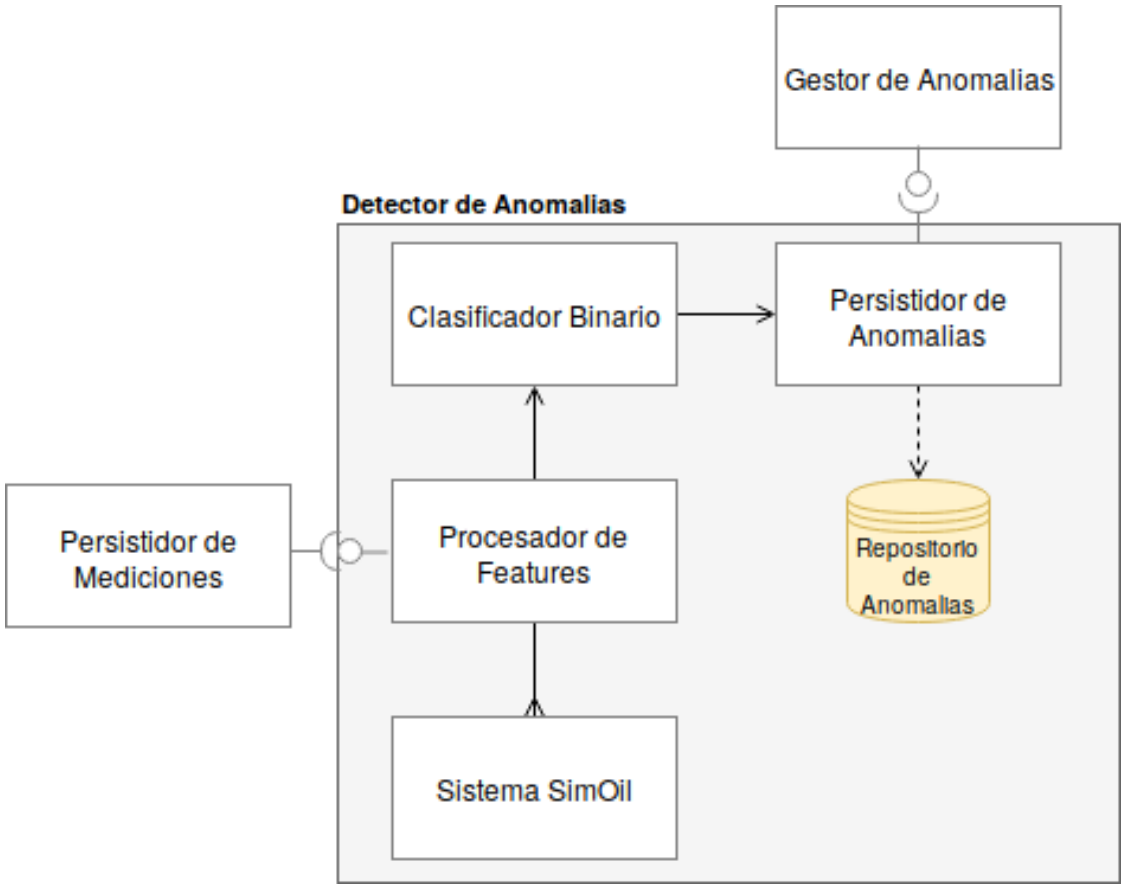

Figura 4: Diagrama de arquitectura del detector de anomalías.

El Detector de Anomalías procesa los datos provistos por el Persistidor de Mediciones, arrancando con el Procesador de Features. Este componente extrae una serie de features o características con la asistencia del Sistema SimOil especificado en el trabajo anterior. Una vez procesados estos datos, se utiliza un clasificador binario (por el momento un modelo Logístico que ya esta entrenado) para definir si el dato procesado es o no una anomalía. En caso de ser una anomalía, se envía al Persistidor de Anomalías para bajar la probabilidad de perdida de datos ante un problema del sistema. Estos datos luego son enviados al Gestor de Anomalías.

3.4. Gestor de anomalias

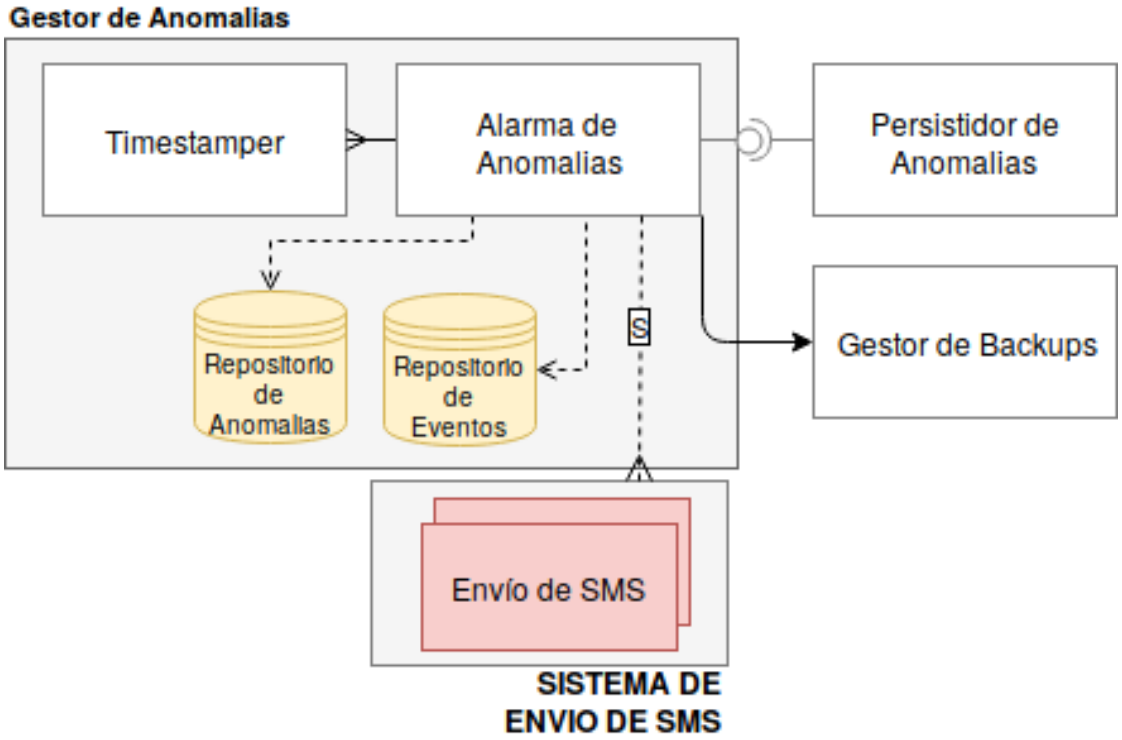

Figura 5: Diagrama de arquitectura del gestor de mediciones.

Al recibir datos de anomalias detectadas desde el Persistidor de Anomalias, la Alarma de Anomalias se ocupa de notificar al Jefe de Operaciones del correspondiente yacimiento de que se ha producido una anomalia. Luego a los datos se les asigna un timestamp y son guardados en el Repositorio de Anomalías y en el Repositorio de Eventos. Para lograr una mayor disponibilidad y tener un sistema tolerante a fallas, los datos sobre anomalías también son enviados a un Gestor de Backups que se ocupa mediante un conjunto de racks de RAIDs para tener mayor redundancia. En caso de falla, los procesos del componente se reinician y buscan los datos sobre las ultimas fallas que han ocurrido y no han sido reportadas desde este repositorio.

Por favor asegurense que esto esta lo mas explicito posible:
1. ¿Cómo se cumplen los requerimientos de disponibilidad?
2. ¿Cómo se cumplen los requerimientos de seguridad?
3. ¿Cómo es la interacción con los servicios externos? (Instrumentos de monitoreo) ¿Hay disponibilidad? ¿Seguridad? ¿Es tolerante a fallos?
4. ¿Cómo se logra performance? ¿Se cumple pronóstico de evento catastrófico 24hs antes?
5. ¿Cómo se informa a los entes reguladores?

4. Conclusiones

EZE Y CHRIS! Por favor relean el TP y fíjense si pueden agregar mas cosas arriba. También vean si pueden escribir esto.

1. Comparar "programming in the smallz "programming in the large"(disenio OO vs Arquitectura)

2. Conclusiones que saco el grupo