

Contrato Interadministrativo Nro. 3021063 De 2021
Suscrito Entre la Empresa de Telecomunicaciones de Bogotá y el Fondo Financiero
Distrital de Salud - Secretaría Distrital de Salud

Fase 3 del Proyecto
Grupo de Entregables E17 – Desarrollo Evolutivo, Parametrización y Pruebas

Requerimientos Pruebas no Funcionales - SISEM

Código:
SISEM-3-E17-5

Bogotá, 22 de noviembre de 2023

FICHA DE IDENTIFICACIÓN DEL DOCUMENTO

Título del Documento	“Requerimientos Pruebas no Funcionales - SISEM”	
Resumen	Este documento presenta el manejo de los requisitos no funcionales asociados al sistema SISEM.	
Código	SISEM-3-E17-5	
Autor	ETB	
Estado	V1 para revisión	22/11/2023
Revisado por		
Aprobado por		

CONTROL DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1	Versión inicial	José Daniel Peña	22/11/2023

DERECHOS DE AUTOR

Derechos de autor
ETB. Todo el material de este entregable puede ser utilizado libremente por la SDS y las personas a quienes está asigne en el marco del convenio citado.

CRÉDITOS

Créditos
Grupo Gestión del Cambio de ETB.

Tabla de Contenido

1. INTRODUCCIÓN	7
2. OBJETIVO	8
3. ALCANCE	9
4. AUDIENCIA.....	10
5. REQUERIMIENTOS DE RENDIMIENTO	11
5.1. TIEMPOS DE RESPUESTA	11
5.1.1. FRONTEND (ANGULAR) - ENTREGA DE INTERFAZ GRÁFICA.....	11
5.1.2. BACKEND (NODE.JS) - PROCESAMIENTO DE DATOS.....	11
5.1.3. CONSULTAS A BASES DE DATOS - LATENCIA DE CONSULTAS	11
5.2. CAPACIDAD DE USUARIOS CONCURRENTES.....	12
5.2.1. ESCALABILIDAD HORIZONTAL Y VERTICAL.....	12
5.2.2. OPTIMIZACIÓN DE CONSULTAS.....	12
5.2.3. CACHÉ DE CONTENIDO ESTÁTICO.....	13
5.2.4. PRUEBAS DE CARGA Y ESTRÉS	13
5.2.5. MONITOREO EN TIEMPO REAL	13
5.2.6. BALANCEO DE CARGA	13
5.2.7. ESCALABILIDAD AUTOMÁTICA.....	13
5.3. CAPACIDAD DE PROCESAMIENTO.....	14
5.4. CONFIGURACIÓN DE RECURSOS	14
5.4.1. OPTIMIZACIÓN DE CÓDIGO	14
5.4.2. PARALELIZACIÓN DE PROCESOS.....	14
5.4.3. MONITORIZACIÓN DEL RENDIMIENTO	14
5.4.4. ESCALABILIDAD VERTICAL Y HORIZONTAL.....	14
5.4.5. PLANIFICACIÓN DE CAPACIDAD FUTURA.....	14
5.4.6. PRUEBAS DE RENDIMIENTO	14
5.5. DISPONIBILIDAD Y TIEMPO DE INACTIVIDAD	16
5.5.1. DISPONIBILIDAD	16
5.5.2. ARQUITECTURA DE ALTA DISPONIBILIDAD	16
5.5.3. RESPUESTA A FALLOS	16
5.5.4. PRUEBAS DE CONFIABILIDAD.....	16
5.5.5. MANTENIMIENTO PROGRAMADO	16
5.5.6. MONITORIZACIÓN PROACTIVA	16
5.5.7. RESPALDO Y RESTAURACIÓN	16
5.5.8. DOCUMENTACIÓN DE PROCEDIMIENTOS DE RECUPERACIÓN.....	16

5.6.	LATENCIA	17
5.6.1.	LATENCIA DE FRONTEND	17
5.6.2.	LATENCIA DE BACKEND.....	17
5.6.3.	LATENCIA DE COMUNICACIÓN ENTRE COMPONENTES	17
5.6.4.	LATENCIA DE RED Y COMUNICACIÓN EXTERNA	17
5.6.5.	LATENCIA GEOGRÁFICA.....	17
5.6.6.	PRUEBAS DE CARGA Y ESTRÉS	17
5.6.7.	MONITOREO CONTINUO	17
6.	REQUERIMIENTOS DE SEGURIDAD	18
6.1.	POLÍTICAS DE ACCESO Y CONTROL	18
6.1.1.	GESTIÓN DE USUARIOS Y ROLES	18
6.1.2.	AUTENTICACIÓN Y AUTORIZACIÓN	18
6.1.3.	POLÍTICAS DE CONTRASEÑAS.....	18
6.1.4.	BLOQUEO DE CUENTAS POR INTENTOS FALLIDOS	19
6.1.5.	REGISTRO DE ACTIVIDADES Y AUDITORÍA	19
6.1.6.	CONTROL DE SESIONES.....	19
6.1.7.	PROTECCIÓN DE DATOS SENSIBLES.....	19
6.1.8.	GESTIÓN DE PERMISOS ESPECIALES	19
6.2.	ENCRIPCIÓN Y PROTECCIÓN DE DATOS.....	19
6.2.1.	ENCRIPCIÓN EN REPOSO.....	19
6.2.2.	ENCRIPCIÓN EN TRÁNSITO	19
6.2.3.	ALMACENAMIENTO SEGURO DE CLAVES.....	19
6.2.4.	PROTECCIÓN CONTRA ATAQUES DE FUERZA BRUTA.....	19
6.2.5.	GESTIÓN DE CERTIFICADOS DIGITALES	20
6.2.6.	SEGMENTACIÓN DE REDES	20
6.2.7.	GESTIÓN DE CLAVES DE ACCESO	20
6.2.8.	AUDITORÍA DE ACCESOS Y USO DE CLAVES.....	20
6.2.9.	PROTECCIÓN CONTRA AMENAZAS INTERNAS	20
6.2.10.	ACTUALIZACIONES Y PARCHES DE SEGURIDAD	20
6.3.	AUDITORÍA Y MONITOREO DE EVENTOS	21
6.4.	GESTIÓN DE IDENTIDAD Y ACCESO	22
7.	REQUERIMIENTOS DE ESCALABILIDAD Y DISPONIBILIDAD.....	23
7.1.	ESCALABILIDAD HORIZONTAL Y VERTICAL	23
7.1.1.	ESCALABILIDAD HORIZONTAL	23
7.1.2.	ESCALABILIDAD VERTICAL.....	23

7.2.	TOLERANCIA A FALLOS Y REDUNDANCIA.....	23
7.2.1.	REDUNDANCIA DE COMPONENTES CRÍTICOS.....	23
7.2.2.	MONITOREO CONTINUO	23
7.2.3.	RESPUESTA AUTOMATIZADA A FALLOS	23
7.2.4.	RESPALDO Y RESTAURACIÓN	24
7.2.5.	PRUEBAS DE RESILIENCIA	24
8.	REQUERIMIENTOS DE USABILIDAD	24
8.1.	INTERFAZ DE USUARIO INTUITIVA	24
8.2.	DOCUMENTACIÓN Y AYUDA CONTEXTUAL.....	24
8.3.	CAPACITACIÓN Y FACILIDAD DE ADOPCIÓN	24
9.	REQUERIMIENTOS DE MANTENIBILIDAD Y SOPORTE.....	25
9.1.	FACILIDAD DE MANTENIMIENTO	25
9.2.	DOCUMENTACIÓN DE CÓDIGO Y ARQUITECTURA	26
9.3.	SOPORTE Y ACTUALIZACIONES FUTURAS	26
10.	REQUERIMIENTOS DE INTEGRACIÓN.....	27
10.1.	INTEGRACIÓN CON OTROS SISTEMA	27
10.1.1.	INTEROPERABILIDAD CON SISTEMAS EXTERNOS.....	27
10.1.2.	COMPATIBILIDAD DE DATOS Y FORMATOS	27
10.1.3.	SEGURIDAD EN LA INTEGRACIÓN.....	27
10.1.4.	GESTIÓN DE ERRORES Y NOTIFICACIONES.....	27
10.2.	CONSISTENCIA DE DATOS	27
10.2.1.	MODELADO DE DATOS UNIFICADO.....	27
10.2.2.	VALIDACIÓN Y NORMALIZACIÓN	27
10.2.3.	TRANSACCIONES Y CONTROL DE LA ATOMICIDAD	28
10.2.4.	SINCRONIZACIÓN Y ACTUALIZACIÓN EN TIEMPO REAL.....	28
10.2.5.	RESOLUCIÓN DE CONFLICTOS Y DUPLICADOS	28
10.3.	CONTROL DE ERRORES Y REINTENTOS	28
10.3.1.	MANEJO DE EXCEPCIONES	28
10.3.2.	REINTENTO AUTOMÁTICO	28
10.3.3.	REGISTRO DE ERRORES	28
10.3.4.	NOTIFICACIONES Y ALERTAS	28
11.	REQUERIMIENTOS DE TRAZABILIDAD Y AUDITORÍA	28
11.1.	TRAZABILIDAD DE EVENTOS.....	29
11.2.	AUDITORÍA DE ACTIVIDADES	29

Tabla de Ilustraciones

ILUSTRACIÓN 1 UBICACIÓN DE LOS SERVIDORES.....	12
ILUSTRACIÓN 2 HERRAMIENTA PRUEBAS DE CAPACIDAD	13
ILUSTRACIÓN 3 RENDIMIENTO CLÚSTER DE PREPRODUCCIÓN	15
ILUSTRACIÓN 4 LATENCIA FRONT END	18
ILUSTRACIÓN 5 CERTIFICADOS DIGITALES.....	21
ILUSTRACIÓN 6 REGISTRO DE EVENTOS	22
ILUSTRACIÓN 7 USABILIDAD	25
ILUSTRACIÓN 8 ACTUALIZACIÓN DE CÓDIGO.....	26

1. Introducción

Los requerimientos no funcionales constituyen una parte fundamental en el diseño y desarrollo del Sistema de Seguimiento y Monitoreo (SISEM). A diferencia de los requerimientos funcionales, que delinean las capacidades y comportamientos específicos del sistema, los no funcionales establecen los criterios que determinan la calidad, eficiencia y seguridad de este. En este documento, se detallan los aspectos clave que abarcan desde el rendimiento y la seguridad hasta la escalabilidad y la usabilidad de SISEM.

Este conjunto de requerimientos no funcionales representa la base sobre la cual se establece un sistema confiable y robusto, capaz de satisfacer las demandas actuales y futuras de los usuarios y las operaciones críticas de seguimiento y monitoreo.

Desde la disponibilidad constante hasta la capacidad de respuesta ágil, cada uno de estos aspectos contribuye a la excelencia operativa y al éxito sostenible del SISEM. A través de un análisis y una especificación clara, se busca garantizar que el sistema cumpla con los estándares más exigentes y brinde una experiencia óptima para todos los involucrados.

2. Objetivo

Definir los parámetros y criterios de calidad: Establecer estándares técnicos y operativos que garanticen la eficiencia, la seguridad, la disponibilidad y la usabilidad del sistema SISEM. Esto implica detallar los límites de rendimiento, las capacidades de escalabilidad, la tolerancia a fallos y otros aspectos clave para satisfacer las necesidades operativas y de los usuarios finales.

Delimitar los aspectos de integración y compatibilidad: Especificar los requisitos de interoperabilidad con otros sistemas, así como los estándares de intercambio de datos y la integración con herramientas y protocolos específicos.

Esto incluye definir la forma en que SISEM interactúa con otras plataformas, sistemas externos y servicios, así mismo internamente con varios componentes internos garantizando la coherencia y la consistencia en el intercambio de información.

3. Alcance

Este documento tiene como objetivo establecer y detallar los criterios de calidad, restricciones técnicas y parámetros operativos que guiarán el desarrollo, despliegue y operación del Sistema de Emergencias Médicas (SISEM). Se centra en los aspectos no funcionales del sistema, abordando áreas como rendimiento, seguridad, disponibilidad, usabilidad, escalabilidad, integración, mantenibilidad, auditoría y otros aspectos clave que no son directamente relacionados con las funciones específicas del sistema, pero que son cruciales para su desempeño global y eficiencia operativa.

El alcance de este documento comprende la identificación y especificación de los requisitos no funcionales que impactan la calidad, operatividad y efectividad del SISEM. Esto incluye, pero no se limita a, establecer los límites de rendimiento, definir medidas de seguridad, establecer directrices para la usabilidad y accesibilidad, describir los mecanismos de integración con otros sistemas, proponer estrategias para garantizar la disponibilidad y la tolerancia a fallos, y abordar consideraciones de mantenibilidad y auditoría.

4. Audiencia

Este documento está dirigido a los usuarios técnicos del sistema, más específicamente a aquellos que se desempeñan en la Dirección de Tecnologías de la Información y la Comunicación – TIC, en su calidad de solicitantes de servicios, procesos, datos, información y demás herramientas funcionales y no funcionales que les debe proveer la solución contratada, en el marco del SISEM.

5. Requerimientos de Rendimiento

Para garantizar una experiencia óptima y eficiente, el sistema SISEM debe cumplir con una serie de requisitos de rendimiento bien definidos. Estos parámetros se centran en la capacidad de respuesta del sistema, su habilidad para manejar cargas de trabajo concurrentes y el tiempo de procesamiento de las operaciones críticas. A continuación, se detallan los requerimientos en esta área:

5.1. Tiempos de Respuesta

Cuando se trata de definir los tiempos de respuesta en un sistema como SISEM, es esencial considerar varios factores, como la ubicación geográfica de los usuarios y los componentes tecnológicos utilizados. Aquí te proporciono una estimación general para los diferentes niveles del sistema:

5.1.1. Frontend (Angular) - Entrega de Interfaz Gráfica

El frontend desarrollado en Angular debería proporcionar una experiencia de usuario fluida, con tiempos de carga de página inferiores a 2 segundos para la mayoría de las vistas, incluso para conexiones desde ubicaciones remotas como Colombia.

Esto se puede lograr mediante técnicas de optimización de código y recursos, así como el uso eficiente de cachés.

5.1.2. Backend (Node.js) - Procesamiento de Datos

El backend, basado en Node.js, debe ser altamente eficiente en el procesamiento de datos. Las operaciones críticas, como la obtención y procesamiento de información de la base de datos, deben tener tiempos de respuesta en el orden de milisegundos para garantizar una experiencia de usuario sin demoras perceptibles.

5.1.3. Consultas a Bases de Datos - Latencia de Consultas

Las consultas a bases de datos alojadas en la región de USA (iowa) deberían tener una latencia baja, preferiblemente inferior a 100 milisegundos. Esto garantiza que la obtención de datos desde la base de datos no sea un cuello de botella en el rendimiento general del sistema.

Estado	Nombre ↑	Zona	Tipo de máquina
✓	analisis-datos	us-east1-b	n1-standard-2
✓	demosidcrue	us-east1-b	custom-1-7680-ext
✓	dev-sisem	us-east1-b	e2-standard-4
✓	gke-sisem-dev-cluster-1-pool-2-c72f7cb9-6yai	us-east1-b	e2-standard-4
✓	gke-sisem-dev-cluster-1-pool-2-c72f7cb9-g975	us-east1-b	e2-standard-4
✓	gke-sisem-dev-cluster-1-pool-2-c72f7cb9-hjy8	us-east1-b	e2-standard-4
✓	gke-sisem-mobile-clu-sisem-mobile-def-3ac97b02-863t	us-east1-b	e2-standard-2
✓	gke-sisem-mobile-clu-sisem-mobile-def-3ac97b02-k8sv	us-east1-b	e2-standard-2
✓	gke-sisem-preprod-cluste-default-pool-2639c9cb-2wgv	us-east1-c	e2-standard-4
✓	gke-sisem-preprod-cluste-default-pool-2639c9cb-bx8o	us-east1-c	e2-standard-4
✓	gke-sisem-preprod-cluste-default-pool-2639c9cb-g934	us-east1-c	e2-standard-4
✓	gke-sisem-qa-cluster-1-default-pool-4cd114a4-fpd5	us-east1-b	e2-standard-4
✓	gke-sisem-qa-cluster-1-default-pool-4cd114a4-jgnl	us-east1-b	e2-standard-4
✓	gke-sisem-qa-cluster-1-default-pool-4cd114a4-w7g4	us-east1-b	e2-standard-4
○	windows-power-bi	us-east1-b	e2-standard-4
○	winserver	us-east1-b	e2-medium

Ilustración 1 Ubicación de los servidores

5.2. Capacidad de Usuarios Concurrentes

La capacidad de usuarios concurrentes es un factor crítico para garantizar un rendimiento óptimo en SISEM. Dado que el cliente ha indicado una necesidad de 200 usuarios simultáneos, es fundamental diseñar la infraestructura y la arquitectura del sistema para satisfacer esta demanda. Aquí, algunas consideraciones:

5.2.1. Escalabilidad Horizontal y Vertical

El sistema está diseñado para escalar tanto horizontal como verticalmente. Esto implica la capacidad de agregar más instancias de servidores y aumentar los recursos de hardware, según sea necesario, para manejar picos de carga de usuarios.

5.2.2. Optimización de Consultas

Las consultas a la base de datos están altamente optimizadas para garantizar respuestas rápidas incluso con una alta carga de usuarios. Índices adecuados, consultas eficientes y cachés de datos son herramientas implementadas.

5.2.3. Caché de Contenido Estático

El sistema entrega contenido estático, como imágenes o archivos CSS/JS, se consideró implementar un mecanismo de caché para reducir la carga en el servidor y acelerar la entrega de estos recursos.

5.2.4. Pruebas de Carga y Estrés

Realiza pruebas exhaustivas de carga y estrés para evaluar cómo el sistema se comporta con 200 usuarios concurrentes y más.

5.2.5. Monitoreo en Tiempo Real

Se implementan herramientas de monitoreo en tiempo real para seguir de cerca la carga del sistema y los tiempos de respuesta. Esto permite tomar medidas preventivas antes de que se alcancen los límites de capacidad.

5.2.6. Balanceo de Carga

El sistema consta de múltiples servidores, se considera implementar un equilibrador de carga para distribuir la carga de manera uniforme entre ellos.

5.2.7. Escalabilidad Automática

también se implementa una solución que permite la escalabilidad automática en función de la carga. Esto garantizará que el sistema pueda adaptarse dinámicamente a los cambios en el número de usuarios concurrentes.

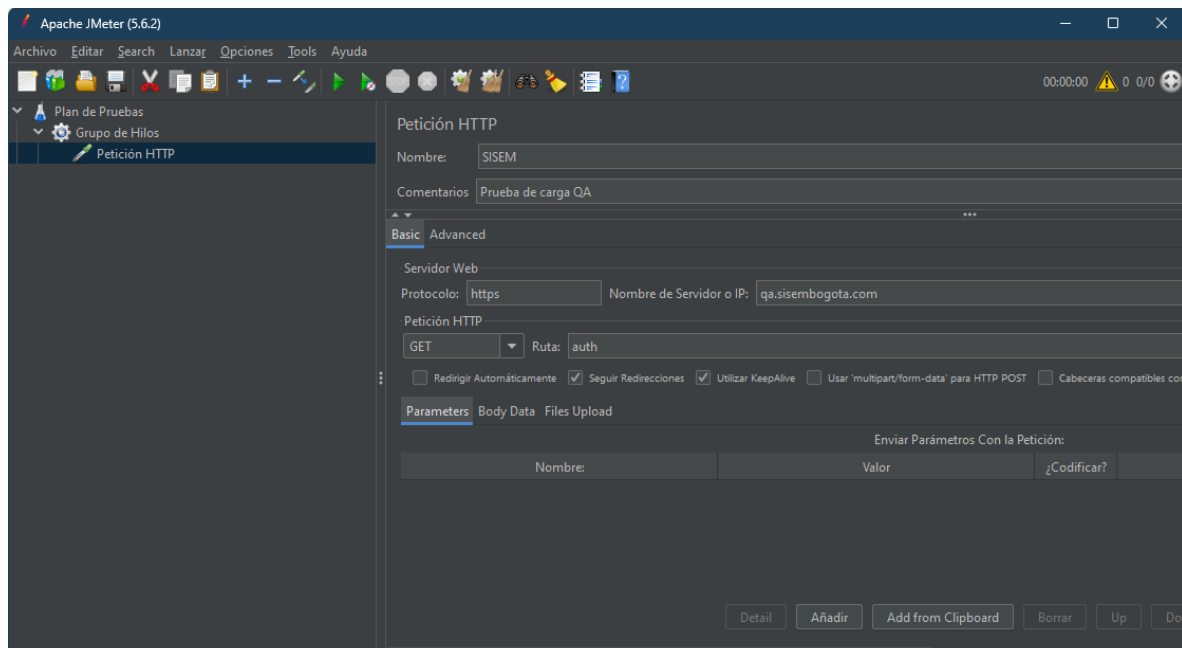


Ilustración 2 Herramienta pruebas de capacidad

5.3. Capacidad de Procesamiento

La capacidad de procesamiento es un componente del sistema SISEM. Dado que el cliente ha indicado una necesidad de soportar alrededor de 200 usuarios simultáneos, es esencial asegurar que la infraestructura y la configuración estén dimensionadas adecuadamente para cumplir con esta demanda. Aquí hay algunas consideraciones sobre la capacidad de procesamiento:

5.4. Configuración de Recursos

Se asegura de que los servidores o contenedores que ejecutan SISEM tengan suficientes recursos de CPU y memoria RAM para manejar la carga esperada. Esto implicó seleccionar instancias de máquinas virtuales o contenedores que cumplan con los requisitos de procesamiento.

5.4.1. Optimización de Código

Se revisa y optimiza el código del sistema para garantizar que las operaciones se ejecuten de manera eficiente y aprovechen al máximo los recursos de procesamiento disponibles (Pruebas unitarias, SONAR). Esto incluye la identificación y corrección de cuellos de botella de rendimiento.

5.4.2. Paralelización de Procesos

Se considera la posibilidad de implementar procesos paralelos para aprovechar al máximo los núcleos de CPU disponibles y acelerar la ejecución de tareas.

5.4.3. Monitorización del Rendimiento

Implementar herramientas de monitorización del rendimiento que permiten realizar un seguimiento de la utilización de CPU en tiempo real. Esto te ayudará a identificar picos de carga y tomar medidas correctivas cuando sea necesario.

5.4.4. Escalabilidad Vertical y Horizontal

Se asegura de que el sistema sea capaz de escalar verticalmente (aumentar la capacidad de los recursos en una sola instancia) y horizontalmente (agregar más instancias: Nodos y Pods) para hacer frente a cargas de trabajo crecientes, sin tener que hacer red despliegues o configuraciones adicionales.

5.4.5. Planificación de Capacidad Futura

Consideración de las necesidades de capacidad futura y se asegura de que la infraestructura sea escalable para acomodar el crecimiento del sistema y las demandas cambiantes del usuario final.

5.4.6. Pruebas de Rendimiento

Se realizaron pruebas de rendimiento exhaustivas para evaluar el comportamiento del sistema bajo cargas de trabajo simuladas y verificar que la capacidad de procesamiento sea suficiente para soportar 200 usuarios simultáneos.

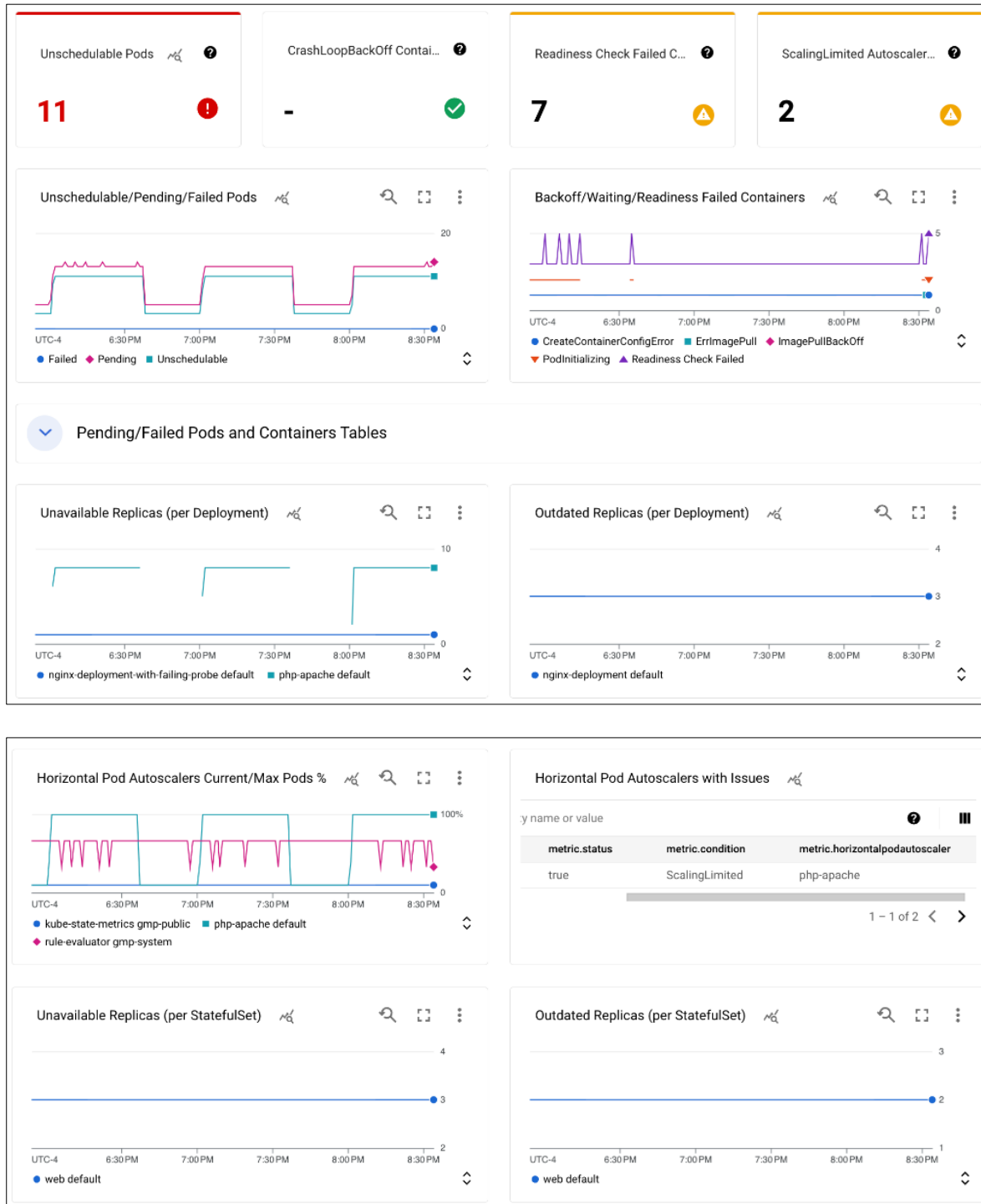


Ilustración 3 Rendimiento clúster de preproducción

5.5. Disponibilidad y Tiempo de Inactividad

La disponibilidad y el tiempo de inactividad se debe tener cuenta a nivel de requerimientos no funcionales, y el SISEM no es la excepción. Algunas consideraciones al respecto:

5.5.1. Disponibilidad

Se establece y se despliega basado en la disponibilidad solicitada contractualmente para el sistema SISEM. Esto significa que el sistema está disponible el 99.95% del tiempo en un período específico.

5.5.2. Arquitectura de Alta Disponibilidad

El diseño la arquitectura de SISEM se definido para tener alta disponibilidad. Esto incluye la implementación de redundancia en componentes críticos, la distribución de carga y la planificación de failovers.

5.5.3. Respuesta a Fallos

Se establecen procedimientos claros para responder a situaciones de fallos. Esto implica la implementación de políticas de recuperación automática y la configuración de alertas para notificar al equipo de operaciones (mesa de servicios) en caso de un problema.

5.5.4. Pruebas de Confiabilidad

Se realizan pruebas de confiabilidad para simular escenarios de fallos y evaluar cómo responde el sistema. Esto incluye pruebas de conmutación por error, pruebas de redundancia y pruebas de recuperación de desastres.

5.5.5. Mantenimiento Programado

Se establecieron ventanas de mantenimiento programado para llevar a cabo actualizaciones y mejoras en el sistema.

5.5.6. Monitorización Proactiva

Implementar herramientas de monitorización proactiva para supervisar el estado del sistema en tiempo real. Esto permitirá identificar posibles problemas antes de que afecten la disponibilidad.

5.5.7. Respaldo y Restauración

Establecer políticas de respaldo y restauración de datos para garantizar que la información crítica esté protegida contra pérdidas. Se realizan pruebas periódicas de restauración para verificar la integridad de los respaldos.

5.5.8. Documentación de Procedimientos de Recuperación

Se documentan y se socializan los procedimientos detallados de recuperación para abordar diferentes tipos de fallos.

5.6. Latencia

La latencia es un aspecto importante en la experiencia del usuario y el rendimiento del sistema. Para el proyecto SISEM, es importante considerar la latencia en varios niveles:

5.6.1. Latencia de Frontend

Se realiza la evaluación de la latencia experimentada por los usuarios al interactuar con la interfaz de usuario. Esto incluye el tiempo que transcurre desde que el usuario realiza una acción hasta que ve la respuesta en la pantalla. Para una aplicación web desarrollada en Angular, la latencia del frontend puede estar influenciada por factores como la carga de recursos, la optimización del código y la eficiencia de las consultas a los servicios backend.

5.6.2. Latencia de Backend

Se examina la latencia en las operaciones y consultas que se realizan en el lado del servidor. Esto incluye consultas a bases de datos, procesamiento de datos y comunicación con otros sistemas o servicios. Es importante optimizar las consultas y procesos para minimizar la latencia y garantizar una respuesta rápida.

5.6.3. Latencia de Comunicación entre Componentes

El sistema SISEM consta de varios componentes o microservicios, es esencial evaluar la latencia en la comunicación entre ellos. Esto implica el uso de herramientas de monitoreo y perfilado para identificar posibles cuellos de botella y mejorar la eficiencia de la comunicación.

5.6.4. Latencia de Red y Comunicación Externa

Considerar la latencia asociada con la comunicación entre el sistema SISEM y otros sistemas externos o servicios de terceros. Esto incluye la integración con servicios de autenticación, APIs de proveedores externos, o cualquier otro tipo de comunicación a través de la red. Es importante validar los servicios y proveedores que ofrezcan baja latencia para mantener un rendimiento óptimo.

5.6.5. Latencia Geográfica

El sistema es accesible desde ubicaciones geográficas diversas, es importante tener en cuenta la latencia que puede surgir debido a la distancia física entre el cliente y el servidor.

5.6.6. Pruebas de Carga y Estrés

Realizar pruebas de carga y estrés para evaluar cómo se comporta el sistema bajo cargas de trabajo intensivas. Esto te permitirá identificar los puntos de estrangulamiento y optimizar el sistema para manejar un mayor volumen de transacciones sin una degradación significativa del rendimiento.

5.6.7. Monitoreo Continuo

Implementar herramientas de monitoreo de latencia en tiempo real para supervisar el rendimiento del sistema en producción. Esto permite identificar y abordar problemas de latencia de manera proactiva.

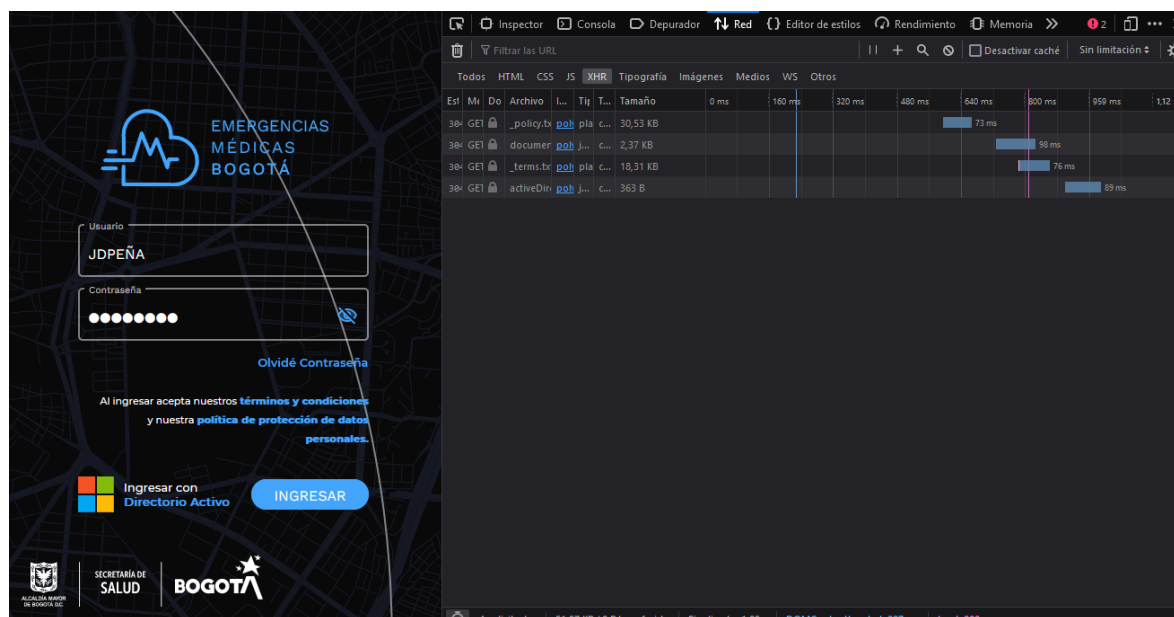


Ilustración 4 Latencia Front End

Optimizar la latencia en todos estos niveles contribuirá a proporcionar una experiencia de usuario fluida y eficiente en el sistema SISEM.

6. Requerimientos de Seguridad

La seguridad es una parte importante fundamental en el diseño y operación del sistema SISEM. Garantizar la protección de la información, la integridad de los datos y la confidencialidad de los usuarios es una prioridad. En este apartado, se detallan los requerimientos de seguridad que se han incorporado en el proyecto para mitigar riesgos y salvaguardar el funcionamiento del sistema.

6.1. Políticas de Acceso y Control

6.1.1. Gestión de Usuarios y Roles

Se implementa un sistema de gestión de usuarios que permite la asignación de roles y privilegios específicos (Keycloak). Cada usuario tiene un perfil definido que determina qué acciones puede realizar y qué datos puede acceder.

6.1.2. Autenticación y Autorización

Se establece un proceso de autenticación SSO para verificar la identidad de los usuarios integrado con el directorio activo de la secretaria. Además, se implementa un sistema de autorización que garantiza que los usuarios solo puedan acceder a los recursos y funciones para los cuales tienen permisos explícitos.

6.1.3. Políticas de Contraseñas

Se requiere el uso de contraseñas seguras que cumplan con ciertos criterios de complejidad. Además, se establece una política de cambio periódico de contraseñas para evitar el uso de credenciales obsoletas.

6.1.4. Bloqueo de Cuentas por Intentos Fallidos

Se implementa un mecanismo de bloqueo de cuentas después de un número especificado de intentos fallidos de inicio de sesión. Esto protege contra intentos de acceso no autorizados.

6.1.5. Registro de Actividades y Auditoría

Se lleva un registro detallado de todas las actividades realizadas por los usuarios, incluidos los intentos de inicio de sesión, modificaciones de datos y accesos a recursos sensibles. Esto permite una supervisión efectiva y la identificación temprana de posibles anomalías.

6.1.6. Control de Sesiones

Se establece un control estricto sobre las sesiones de usuario para evitar accesos simultáneos desde múltiples dispositivos o ubicaciones. Las sesiones inactivas se cierran automáticamente después de un período predefinido.

6.1.7. Protección de Datos Sensibles

Se implementan medidas de encriptación y restricciones de acceso adicionales para proteger la confidencialidad de los datos sensibles, como información de salud o datos personales.

6.1.8. Gestión de Permisos Especiales

Se define un proceso para otorgar y revocar permisos especiales, como privilegios de administrador, de manera controlada y documentada.

6.2. Encriptación y Protección de Datos

6.2.1. Encriptación en Reposo

Todos los datos almacenados en bases de datos, sistemas de archivos y otros repositorios son encriptados utilizando algoritmos seguros. Esto asegura que incluso si los datos son comprometidos, no pueden ser leídos sin la clave de descryptación correspondiente.

6.2.2. Encriptación en Tránsito

Se implementa el uso de conexiones seguras (HTTPS) para la transmisión de datos entre el cliente y el servidor. Esto protege la información contra interceptaciones malintencionadas durante la comunicación.

6.2.3. Almacenamiento Seguro de Claves

Las claves de encriptación y descryptación se almacenan de manera segura utilizando soluciones de gestión de claves (GCP), asegurando que solo usuarios autorizados tengan acceso a estas claves críticas.

6.2.4. Protección contra Ataques de Fuerza Bruta

Se implementan medidas para prevenir y detectar intentos de ataques de fuerza bruta, los cuales buscan descifrar las claves de encriptación a través de repetidos intentos.

6.2.5. Gestión de Certificados Digitales

Se realiza la solicitud a secretaria generar los certificados autorizados para dominios gubernamentales, así como indicar el dominio de este sistema.

6.2.6. Segmentación de Redes

Se configura una arquitectura de red que aísla los sistemas sensibles del acceso no autorizado y de redes públicas.

6.2.7. Gestión de Claves de Acceso

Se implementa una política estricta de manejo y rotación de contraseñas y claves de acceso a sistemas y bases de datos.

6.2.8. Auditoría de Accesos y Uso de Claves

Se lleva a cabo una auditoría regular para verificar y rastrear el acceso a claves y la utilización de mecanismos de encriptación.

6.2.9. Protección contra Amenazas Internas

Se implementan medidas para detectar y prevenir amenazas internas, incluido el acceso no autorizado por parte de empleados o usuarios con privilegios elevados.

6.2.10. Actualizaciones y Parches de Seguridad

Se mantiene actualizado el software y se aplican parches de seguridad para mitigar vulnerabilidades conocidas (imágenes de los contenedores).

qa.sisembogota.com		R3	ISRG Root X1
Nombre del asunto			
Nombre común	qa.sisembogota.com		
Nombre del emisor			
País	US		
Organización	Let's Encrypt		
Nombre común	R3		
Validez			
No antes	Sun, 19 Nov 2023 10:48:43 GMT		
No después	Sat, 17 Feb 2024 10:48:42 GMT		
Nombres alternativos del sujeto			
Nombre de la DNS	qa.sisembogota.com		
Información de clave pública			
Algoritmo	RSA		
Tamaño de la clave	2048		
Exponente	65537		
Módulo	C9:3E:B2:DB:B4:AA:FE:91:62:A4:47:BC:C3:00:79:83:74:A5:53:31:69:A9:AA:41:7E:7F...		

Ilustración 5 Certificados digitales

6.3. Auditoría y Monitoreo de Eventos

Se establece un sistema de auditoría que registra y supervisa todas las actividades relevantes en el sistema utilizando el componente de ELK (Elasticsearch, Logstash, Kibana). Esto incluye acciones como accesos, modificaciones de datos, intentos de acceso no autorizado y otros eventos críticos.

Los registros de auditoría son almacenados de manera segura y son accesibles solo para personal autorizado. Además, se implementan medidas para garantizar la integridad y disponibilidad de estos registros.

Se configuran alertas y notificaciones para eventos que requieren atención inmediata, lo que permite una respuesta proactiva ante posibles amenazas o incidentes de seguridad.

Se realiza un monitoreo continuo de los registros de auditoría para identificar patrones o tendencias que puedan indicar posibles brechas de seguridad o actividades sospechosas.

Adicionalmente, se lleva a cabo un análisis periódico de los eventos registrados con el fin de mejorar la seguridad y optimizar los procesos de respuesta a incidentes. Esto incluye la revisión de políticas de acceso, permisos y configuraciones de seguridad.

6.4. Gestión de Identidad y Acceso

Se implementa un sistema de gestión de identidad y acceso robusto que garantiza la autenticación y autorización adecuada de los usuarios. Esto incluye la verificación de credenciales, como contraseñas o autenticación de dos factores.

Se establecen políticas de contraseñas sólidas y se requiere el cambio periódico de las mismas para mantener la seguridad de las cuentas de usuario.

Se asignan roles y permisos de manera granular, asegurando que cada usuario tenga acceso solo a las funciones y datos necesarios para cumplir con sus responsabilidades.

La gestión de identidad y acceso incluye la administración de cuentas de usuario, la creación y desactivación de perfiles, así como la revisión y auditoría de permisos de manera regular.

Se implementa un mecanismo de cierre de sesión automático para prevenir accesos no autorizados por periodos prolongados de inactividad.

Además, se establece un protocolo de respuesta a incidentes de seguridad que incluye la revocación inmediata de accesos en caso de sospecha o confirmación de actividades maliciosas.

La gestión de identidad y acceso se adhiere a estándares de seguridad reconocidos, garantizando la protección de los datos y la confidencialidad de la información.

SEVERIDAD	MARCA DE TIEMPO	RESUMEN
> *	2023-11-20 18:10:56.846 EST	Kubernetes Apiservice Requests update kube-system/cloud-controller-manager system:cloud-controller-manager (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, auth...
> *	2023-11-20 18:10:56.168 EST	Kubernetes Apiservice Requests update kube-system/gcp-controller-manager system:gcp-controller-manager (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authoriz...
> *	2023-11-20 18:10:56.317 EST	Kubernetes Apiservice Requests update kube-system/ingress-gce-lock system:l7-lb-controller (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizationInfo: [...
> *	2023-11-20 18:10:56.861 EST	Kubernetes Apiservice Requests update sisen-pre-prod/ingress-controller-lea... system:serviceaccount:sisen-pre-prod:... (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo:...
> *	2023-11-20 18:10:56.871 EST	Kubernetes Apiservice Requests update sisen-pre-prod/ingress-controller-lea... system:serviceaccount:sisen-pre-prod:... (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo:...
> *	2023-11-20 18:10:56.915 EST	Kubernetes Apiservice Requests update kube-system/cluster-autoscaler system:cluster-autoscaler (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizationInf...
> *	2023-11-20 18:10:56.977 EST	Kubernetes Apiservice Requests update kube-system/kube-scheduler system:kube-scheduler (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizationInfo: [], ...
> *	2023-11-20 18:10:57.234 EST	Kubernetes Apiservice Requests update kube-system/cloud-provider-extraction... system:cloud-controller-manager (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, au...
> *	2023-11-20 18:10:57.385 EST	Kubernetes Apiservice Requests update kube-system/cluster-kubestore system:kubestore-collector (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizationInf...
> *	2023-11-20 18:10:57.580 EST	Kubernetes Apiservice Requests update kube-system/managed-certificate-contr... system:managed-certificate-controller (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizat...
> *	2023-11-20 18:10:58.535 EST	Kubernetes Apiservice Requests update kube-system/gke-common-webhook-lock system:gke-common-webhooks (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizat...
> *	2023-11-20 18:10:57.996 EST	Kubernetes Apiservice Requests update kube-system/addon-manager system:addon-manager (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizationInfo: [], me...
> *	2023-11-20 18:10:58.528 EST	Kubernetes Apiservice Requests update kube-system/vpa-recommender system:vpa-recommender (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizationInfo: [], ...
> *	2023-11-20 18:10:58.535 EST	Kubernetes Apiservice Requests update kube-system/vpa-recommender system:vpa-recommender (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizationInfo: [], ...
> *	2023-11-20 18:10:59.254 EST	Kubernetes Apiservice Requests update kube-system/snapshot-controller-leader system:snapshot-controller (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authori...
> *	2023-11-20 18:10:59.588 EST	Kubernetes Apiservice Requests update kube-system/managed-certificate-contr... system:managed-certificate-controller (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizat...
> *	2023-11-20 18:10:59.990 EST	Kubernetes Apiservice Requests update kube-system/gke-common-webhook-lock system:gke-common-webhooks (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizat...
> *	2023-11-20 18:11:00.005 EST	Kubernetes Apiservice Requests update kube-system/addon-manager system:addon-manager (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizationInfo: [], me...
> *	2023-11-20 18:11:01.483 EST	Kubernetes Apiservice Requests update kube-system/cluster-kubestore system:kubestore-collector (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizationInf...
> *	2023-11-20 18:11:01.597 EST	Kubernetes Apiservice Requests update kube-system/managed-certificate-contr... system:managed-certificate-controller (@type: type.googleapis.com/google.cloud.audit.AuditLog, authenticationInfo: { }, authorizat...

Ilustración 6 Registro de eventos

7. Requerimientos de Escalabilidad y Disponibilidad

La escalabilidad y disponibilidad del sistema son aspectos fundamentales para garantizar su eficiencia y confiabilidad en entornos de alta demanda. En este sentido, se establecen requerimientos que permiten al sistema adaptarse a un crecimiento orgánico de usuarios y cargas de trabajo, así como asegurar su disponibilidad ininterrumpida en todo momento. A continuación, detallamos los elementos clave en este ámbito.

7.1. Escalabilidad Horizontal y Vertical

La escalabilidad del sistema SISEM se aborda mediante dos enfoques distintos: la escalabilidad horizontal y la vertical.

7.1.1. Escalabilidad Horizontal

Se refiere a la capacidad de distribuir la carga de trabajo a través de múltiples instancias o servidores, permitiendo así manejar un mayor número de solicitudes concurrentes. En el caso de SISEM, se ha diseñado para escalar horizontalmente de manera eficiente, lo que significa que puede adaptarse a incrementos en la demanda sin sacrificar el rendimiento.

7.1.2. Escalabilidad Vertical

Implica la capacidad de mejorar el rendimiento de una instancia o servidor individual mediante la adición de recursos como CPU, RAM o almacenamiento. Si bien SISEM es capaz de aprovechar esta forma de escalabilidad, se ha priorizado la escalabilidad horizontal para brindar una solución más flexible y resiliente a medida que la plataforma crece.

Estos enfoques combinados aseguran que el sistema pueda enfrentar un aumento sostenido en la demanda, así como gestionar picos de tráfico sin comprometer su rendimiento y disponibilidad.

7.2. Tolerancia a Fallos y Redundancia

La arquitectura de SISEM está diseñada para garantizar una alta disponibilidad y tolerancia a fallos. Se implementan diversas estrategias para minimizar el impacto de posibles fallos en el sistema:

7.2.1. Redundancia de Componentes Críticos

Los componentes esenciales del sistema, como la base de datos y los servicios principales, están configurados con replicación y mecanismos de failover. Esto garantiza que, en caso de una falla, otro componente tome el control sin interrupciones en el servicio.

7.2.2. Monitoreo Continuo

Se implementa un sistema de monitoreo en tiempo real que supervisa la salud de los diferentes componentes del sistema.

Cualquier anomalía o falla es detectada y notificada inmediatamente al equipo de operaciones (mesa de ayuda: nivel 1) para una intervención rápida.

7.2.3. Respuesta Automatizada a Fallos

Se han establecido procedimientos automatizados para abordar posibles fallos de forma

inmediata. Esto incluye la capacidad de reiniciar servicios, redireccionar tráfico y realizar cambios en la configuración en tiempo real.

7.2.4. Respaldo y Restauración

Se realizan copias de seguridad periódicas de la base de datos y la configuración del sistema. En caso de una falla catastrófica, se puede restaurar el sistema a un estado funcional previo.

7.2.5. Pruebas de Resiliencia

Se realizan pruebas regulares de tolerancia a fallos para asegurar que el sistema pueda recuperarse de manera efectiva y sin pérdida de datos en situaciones adversas.

8. Requerimientos de Usabilidad

Los requerimientos de usabilidad nos aseguran que el sistema no solo funcione correctamente, sino que también sea fácil de usar y se adapte a las necesidades de los usuarios finales. Estos requerimientos se centran en la experiencia del usuario, buscando proporcionar interfaces intuitivas, accesibles y eficientes. En este apartado, se detallarán los requerimientos que buscan mejorar la experiencia del usuario en el sistema SISEM, asegurando su facilidad de uso, accesibilidad y eficiencia en todas las interacciones.

8.1. Interfaz de Usuario Intuitiva

Una interfaz de usuario intuitiva es fundamental en SISEM para garantizar que los usuarios puedan navegar y utilizar el sistema de manera eficiente desde el primer momento. Esto implica presentar una estructura clara y coherente, con menús y opciones de navegación lógicas, así como elementos visuales comprensibles y consistentes en toda la plataforma.

Los formularios y campos deben ser fáciles de completar, con etiquetas claras y concisas que guíen al usuario durante la interacción. Además, la disposición de los elementos y la organización de la información deben estar diseñadas de manera que reflejen las tareas y flujos de trabajo comunes de los usuarios, facilitando su comprensión y agilizando su realización.

En resumen, la interfaz de SISEM se orienta hacia la simplicidad y la facilidad de uso, priorizando la experiencia del usuario para que pueda realizar sus funciones de manera intuitiva y efectiva.

8.2. Documentación y Ayuda Contextual

SISEM se destaca por su amplia documentación y ayuda contextual, elementos esenciales para brindar soporte a los usuarios y optimizar su experiencia. La documentación detallada proporciona guías paso a paso, manuales de usuario y material instructivo que cubre todos los aspectos del sistema, desde las funcionalidades básicas hasta las más avanzadas. Esta documentación está diseñada para ser accesible y comprensible, adaptándose a distintos niveles de habilidad y conocimiento de los usuarios, para esto de disponibilidad el módulo de ayuda en línea asociado a la comunicación con el sistema del LMS (Moodle).

8.3. Capacitación y Facilidad de Adopción

SISEM se distingue por su enfoque integral en la capacitación y la facilidad de adopción para los usuarios. El sistema ofrece programas de capacitación estructurados y adaptados a las necesidades de diferentes usuarios, desde los nuevos hasta los experimentados. Estos

programas abarcan desde sesiones de capacitación presenciales hasta material educativo en línea, cubriendo tanto aspectos generales del sistema como características más avanzadas.

La facilidad de adopción de SISEM se refleja en su diseño intuitivo y en la disposición de recursos que simplifican la curva de aprendizaje. Además, se han implementado herramientas interactivas, guías visuales y ayudas contextuales para facilitar la navegación y el uso del sistema, lo que reduce la necesidad de una capacitación extensiva para comenzar a utilizar SISEM de manera efectiva. Esta combinación de capacitación estructurada y una interfaz amigable contribuye significativamente a la rápida adopción y dominio del sistema por parte de los usuarios.

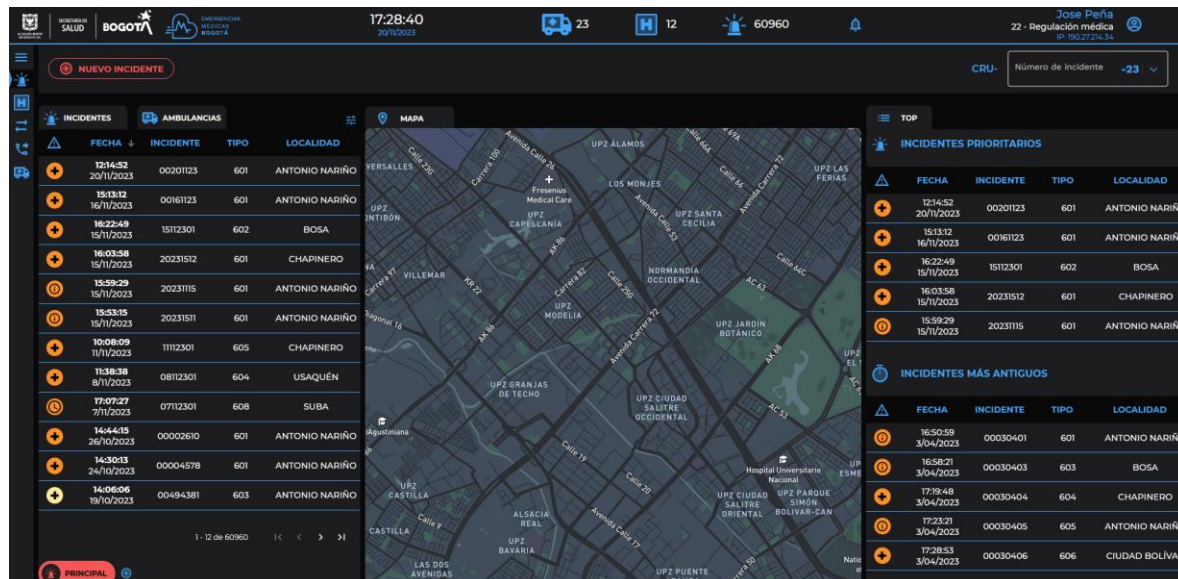


Ilustración 7 Usabilidad

9. Requerimientos de Mantenibilidad y Soporte

Para asegurar la continuidad operativa y la evolución efectiva del sistema SISEM, se han establecido requerimientos de mantenibilidad y soporte que garantizan la estabilidad, la actualización continua y la resolución eficiente de problemas. Estos aspectos son fundamentales para mantener la funcionalidad, la seguridad y la efectividad del sistema a lo largo del tiempo. A continuación, se detallan los requerimientos que abordan la mantenibilidad y el soporte de SISEM, considerando tanto las necesidades técnicas como las operativas para un mantenimiento fluido y una asistencia ágil ante eventualidades.

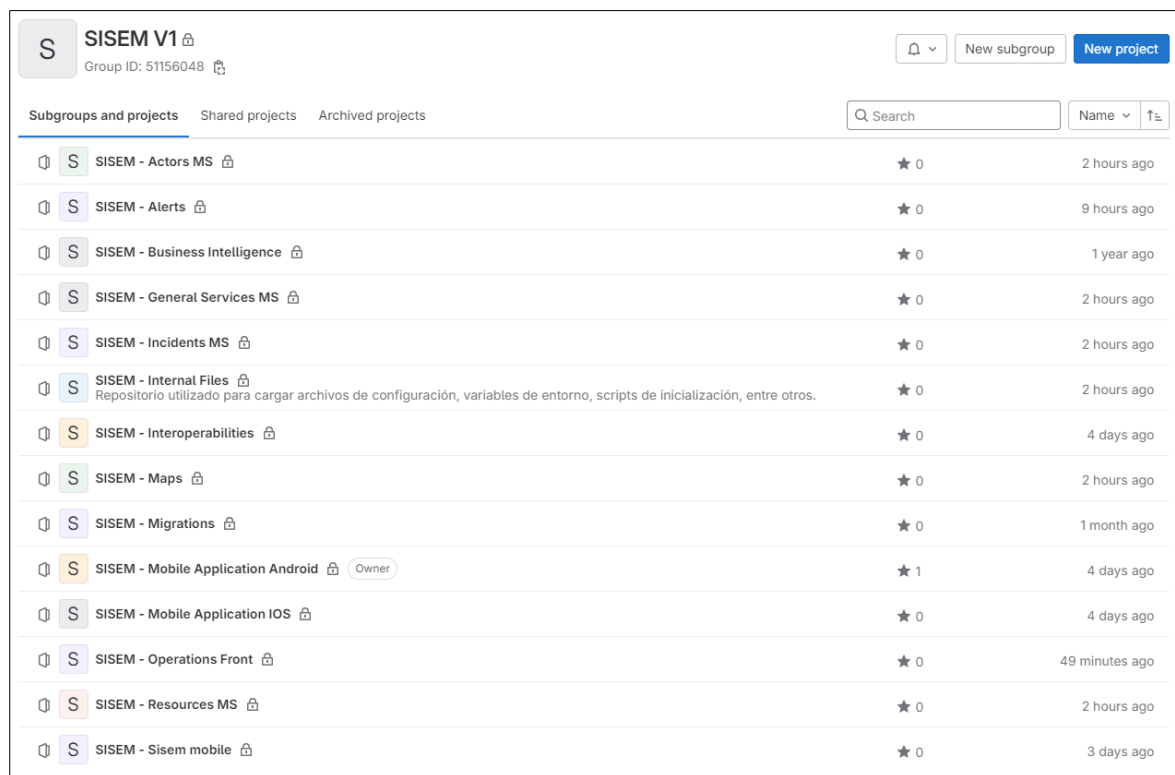
9.1. Facilidad de Mantenimiento

La facilidad de mantenimiento en SISEM se fundamenta en una arquitectura modular y bien estructurada que simplifica las tareas de actualización y corrección.

Este sistema se ha diseñado considerando la separación de componentes, lo que permite intervenir en áreas específicas sin afectar el conjunto completo. Además, la codificación limpia y documentada, junto con el uso de estándares de desarrollo, facilita la comprensión y modificación del código para futuras mejoras o correcciones. El acceso a herramientas de monitoreo y registro de errores también contribuye a una rápida identificación de fallos, lo que agiliza el proceso de mantenimiento y asegura una respuesta ágil ante posibles inconvenientes.

9.2. Documentación de Código y Arquitectura

La documentación de código y arquitectura en SISEM es amplia y bien estructurada. Cada módulo y componente del sistema está acompañado de documentación detallada que describe su funcionamiento, propósito y relaciones con otros elementos del sistema. Esta documentación incluye diagramas de arquitectura, flujos de datos, modelos de bases de datos y explicaciones detalladas de los procesos internos. Además, se sigue un estándar de comentarios en el código que facilita la comprensión de las funciones, métodos y variables utilizadas. Esta documentación es decisiva para nuevos desarrolladores que se unan al proyecto, permitiéndoles familiarizarse rápidamente con la estructura y el funcionamiento del sistema.



The screenshot shows the 'SISEM V1' project page. At the top, there's a header with the project name 'SISEM V1', a group ID '51156048', and buttons for 'New subgroup' and 'New project'. Below the header, there are tabs for 'Subgroups and projects', 'Shared projects', and 'Archived projects'. A search bar and a 'Name' dropdown are also present. The main content is a list of subgroups and projects, each with a folder icon, a name, a star icon with a count, and a timestamp.

Icon	Name	Star Count	Timestamp
📁	SISEM - Actors MS	★ 0	2 hours ago
📁	SISEM - Alerts	★ 0	9 hours ago
📁	SISEM - Business Intelligence	★ 0	1 year ago
📁	SISEM - General Services MS	★ 0	2 hours ago
📁	SISEM - Incidents MS	★ 0	2 hours ago
📁	SISEM - Internal Files Repositorio utilizado para cargar archivos de configuración, variables de entorno, scripts de inicialización, entre otros.	★ 0	2 hours ago
📁	SISEM - Interoperabilities	★ 0	4 days ago
📁	SISEM - Maps	★ 0	2 hours ago
📁	SISEM - Migrations	★ 0	1 month ago
📁	SISEM - Mobile Application Android (Owner)	★ 1	4 days ago
📁	SISEM - Mobile Application IOS	★ 0	4 days ago
📁	SISEM - Operations Front	★ 0	49 minutes ago
📁	SISEM - Resources MS	★ 0	2 hours ago
📁	SISEM - Sisem mobile	★ 0	3 days ago

Ilustración 8 Actualización de código

9.3. Soporte y Actualizaciones Futuras

SISEM cuenta con un compromiso sólido de soporte continuo y actualizaciones futuras. El equipo responsable de su mantenimiento se dedica a brindar asistencia oportuna en caso de problemas o consultas. Además, se siguen prácticas de desarrollo ágiles que permiten la incorporación regular de actualizaciones, mejoras y correcciones de errores. Existe un calendario de actualizaciones planificadas para garantizar que el sistema esté siempre alineado con los requisitos cambiantes del entorno. Esta estrategia asegura que SISEM no solo sea confiable en su desempeño actual, sino que también esté preparado para evolucionar y adaptarse a futuras demandas y avances tecnológicos.

10. Requerimientos de Integración

La integración de sistemas es un aspecto clave en el funcionamiento eficiente de SISEM. Este apartado se centra en los requisitos que garantizan la conectividad, la interoperabilidad y la colaboración sin inconvenientes con otros sistemas y servicios.

La capacidad de SISEM para integrarse de manera efectiva y segura con sistemas externos es fundamental para la optimización de flujos de datos, la mejora de la experiencia del usuario y la eficiencia operativa en un ecosistema informático más amplio.

10.1. Integración con Otros Sistema

La integración de SISEM con otros sistemas es fundamental para garantizar su funcionalidad y utilidad en un entorno más amplio. Aquí algunas áreas relevantes que podrías abordar:

10.1.1. Interoperabilidad con Sistemas Externos

Destaca cómo SISEM puede comunicarse y compartir datos con otros sistemas, ya sea a través de APIs, servicios web u otros mecanismos de integración (Bus de interoperabilidad).

10.1.2. Compatibilidad de Datos y Formatos

SISEM permite trabajar con diferentes formatos de datos y protocolos estándar utilizados en el contexto de la salud y la gestión de emergencias (HL7).

10.1.3. Seguridad en la Integración

Permite la integración utilizando: autenticación, autorización y cifrado de datos para proteger la información confidencial durante la transferencia entre sistemas.

10.1.4. Gestión de Errores y Notificaciones

SISEM maneja situaciones de errores durante la integración y se notifican y registran estas incidencias para su posterior análisis y resolución (Análisis de: Solicitudes y respuestas sobre mongoDB).

10.2. Consistencia de Datos

La consistencia de datos en SISEM es crucial para asegurar la veracidad y coherencia de la información manejada en el sistema. Aquí algunas consideraciones:

10.2.1. Modelado de Datos Unificado

SISEM emplea un modelo de datos cohesivo y unificado que garantiza la consistencia entre las distintas entidades y atributos almacenados. Esto permite una visión integral de la información relacionada con la gestión de emergencias y la atención médica.

10.2.2. Validación y Normalización

En SISEM se valida y normaliza los datos ingresados. Esto incluye la verificación de formatos, integridad y coherencia de la información, lo que minimiza errores y garantiza la uniformidad en los datos almacenados.

10.2.3. Transacciones y Control de la Atomicidad

En SISEM se manejan las transacciones de datos para asegurar la atomicidad, consistencia, aislamiento y durabilidad (propiedades ACID) en las operaciones de lectura y escritura. Esto evita escenarios donde los datos quedan en un estado intermedio o inconsistente.

10.2.4. Sincronización y Actualización en Tiempo Real

SISEM se sincronizan y actualizan los datos en tiempo real entre diferentes módulos o sistemas conectados. Esto asegura que la información crítica esté siempre actualizada y disponible para su uso oportuno.

10.2.5. Resolución de Conflictos y Duplicados

En SISEM se identifican y resuelven conflictos de datos, como duplicados o discrepancias, asegurando que la información se mantenga coherente y precisa en todo momento, incluso en entornos donde múltiples sistemas pueden actualizar la misma información (Premier One).

10.3. Control de Errores y Reintentos

El control de errores y reintentos en SISEM es esencial para garantizar la confiabilidad y la continuidad de las operaciones en entornos donde pueden surgir interrupciones o fallas. Aquí algunos aspectos a considerar:

10.3.1. Manejo de Excepciones

SISEM cuenta con una estructura robusta para el manejo de excepciones. Detecta y registra errores en tiempo real, lo que permite una rápida identificación y respuesta a posibles problemas.

10.3.2. Reintento Automático

En caso de fallos temporales o conexiones intermitentes, SISEM implementa mecanismos de reintentos automáticos.

Esto asegura que las operaciones críticas se ejecuten adecuadamente una vez restaurada la conectividad o resueltos los problemas temporales (Aplicación móvil).

10.3.3. Registro de Errores

SISEM registra y documenta detalladamente los errores ocurridos durante las operaciones. Estos registros proporcionan información valiosa para el análisis y la mejora continua del sistema.

10.3.4. Notificaciones y Alertas

El sistema está configurado para emitir notificaciones y alertas inmediatas cuando se producen errores críticos o fallas, lo que permite una respuesta inmediata por parte del equipo de soporte técnico (mesa de ayuda: nivel 1).

11. Requerimientos de Trazabilidad y Auditoría

Los requerimientos de trazabilidad y auditoría en SISEM son fundamentales para garantizar la transparencia, la integridad y la verificación de las operaciones realizadas en el sistema. La capacidad de rastrear y registrar cada acción, junto con la posibilidad de auditar estos registros. Aquí se detallan los aspectos claves de la trazabilidad y la auditoría en SISEM.

11.1. Trazabilidad de Eventos

La trazabilidad de eventos en SISEM se centra en la capacidad del sistema para registrar y seguir la secuencia de acciones y eventos que ocurren durante el proceso de atención de emergencias médicas. Cada interacción, modificación de estado o respuesta del sistema queda registrada de manera detallada, lo que permite reconstruir la secuencia de eventos en cualquier momento. Esta trazabilidad facilita la revisión posterior de actividades, la identificación de posibles errores o mejoras en el proceso, y asegura la transparencia en la gestión de incidentes médicos.

11.2. Auditoría de Actividades

La auditoría de actividades en SISEM se enfoca en la supervisión y registro detallado de las acciones realizadas por los usuarios dentro del sistema. Esto incluye la creación, modificación o eliminación de registros, accesos a funcionalidades críticas, cambios en el estado de los incidentes, entre otros eventos relevantes. La finalidad es mantener un registro integral de las interacciones de los usuarios con el sistema para garantizar la integridad de los datos, la transparencia en las operaciones y el cumplimiento de normativas. Esta funcionalidad de auditoría permite un seguimiento exhaustivo de las actividades realizadas, facilitando la identificación de cualquier anomalía, el análisis forense en caso de incidentes y la trazabilidad en la gestión de los casos de emergencia médica.