

**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 E20 – Infraestructura, Soporte, Mantenimiento y Operación**

**Actividades realizadas durante el contrato.**

**Código:**  
**SISEM-3-E20-7**

**Bogotá D.C. 25 de agosto de 2025**

**FICHA DE IDENTIFICACIÓN DEL DOCUMENTO**

|                             |                                                                                                                                                                                                                                                                      |            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Título del Documento</b> | <b>“Actividades realizadas durante el contrato”</b>                                                                                                                                                                                                                  |            |
| <b>Resumen</b>              | Este documento presenta las actividades generales realizadas durante la vigencia del contrato, contenidas en mayor detalle en los documentos que hacen parte del entregable, de los cuales se indica el repositorio que los contiene y las recomendaciones a seguir. |            |
| <b>Código</b>               | SISEM-3-E20-7                                                                                                                                                                                                                                                        |            |
| <b>Autor</b>                | ETB                                                                                                                                                                                                                                                                  |            |
| <b>Estado</b>               | V1                                                                                                                                                                                                                                                                   | 25/07/2025 |
| <b>Revisado por</b>         |                                                                                                                                                                                                                                                                      |            |

**CONTROL DE CAMBIOS**

| <b>Versión</b> | <b>Causa del Cambio</b> | <b>Responsable del Cambio</b> | <b>Fecha del Cambio</b> |
|----------------|-------------------------|-------------------------------|-------------------------|
| V1             | Versión inicial         | Carlos Caicedo                | 25/07/2025              |
|                |                         |                               |                         |
|                |                         |                               |                         |
|                |                         |                               |                         |

**DERECHOS DE AUTOR**

|                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Derechos de autor</b>                                                                                                                                 |
| ETB. Todo el material de este entregable puede ser utilizado libremente por la SDS y las personas a quienes ésta asigne en el marco del convenio citado. |

**CRÉDITOS**

|                                           |
|-------------------------------------------|
| <b>Créditos</b>                           |
| Grupos de Diseño de Arquitecturas de ETB. |

## Tabla de Contenido

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| 1. Introducción.....                                                                                        | 5  |
| 2. Alcance.....                                                                                             | 6  |
| 3. Audiencia .....                                                                                          | 7  |
| 4. Definiciones y Conceptos .....                                                                           | 8  |
| 5. Actividades Generales Realizadas .....                                                                   | 9  |
| 6. Operación y Mantenimiento .....                                                                          | 11 |
| 7. Recuperación de Desastres .....                                                                          | 12 |
| 8. Mesa de Ayuda 7x24 (Nivel 1, 2 y 3) y ANS.....                                                           | 14 |
| 9. Aprovisionamiento, Despliegue y Configuración de Infraestructura de Nuevos<br>Desarrollos.....           | 16 |
| 10. Despliegue y Configuración de Infraestructura de Ambiente de Producción de<br>Nuevos Desarrollos.....   | 17 |
| 11. Documentos entregados Entregable E20 – Infraestructura, Soporte, Mantenimiento y<br>Operación 2023..... | 19 |
| 12. Recomendaciones para la Administración y Soporte de la Infraestructura.....                             | 20 |

### Tabla de Ilustraciones

|                                                           |    |
|-----------------------------------------------------------|----|
| Ilustración 1. Documentos entregable E20.....             | 20 |
| Ilustración 2. Documentos Entregable E20, carpeta V2..... | 20 |

## 1. Introducción

El presente documento consolida y describe de manera estructurada las **actividades generales realizadas durante la vigencia del contrato** suscrito para el fortalecimiento, operación y mantenimiento del Sistema de Emergencias Médicas – SISEM. Dichas actividades se desarrollaron en cumplimiento de los lineamientos técnicos, administrativos y contractuales definidos por la Secretaría Distrital de Salud y abarcan desde la planeación estratégica de la infraestructura tecnológica hasta la puesta en producción de nuevos desarrollos, la atención de incidentes y la definición de planes de contingencia.

El documento se soporta en los entregables que conforman el **E20 – Infraestructura, Soporte, Mantenimiento y Operación fase 3**, dentro de los cuales se incluyen planes, configuraciones, procedimientos operativos y reportes asociados a la gestión de la plataforma. Cada entregable presenta un nivel de detalle específico respecto a las actividades realizadas, su metodología de implementación y los resultados alcanzados.

De igual manera, se indica el repositorio en el cual se encuentran los documentos técnicos de referencia, así como las recomendaciones y buenas prácticas a seguir para garantizar la continuidad, seguridad y escalabilidad de la solución tecnológica. Con ello se busca aportar trazabilidad, transparencia y un marco claro de operación que permita la evolución del SISEM en el mediano y largo plazo.

## 2. Alcance

El alcance del presente documento comprende la recopilación, descripción y análisis de las actividades ejecutadas durante la vigencia contractual en el marco del **E20 – Infraestructura, Soporte, Mantenimiento y Operación fase 3**, las cuales se encuentran documentadas en los siguientes entregables:

- **E20-1:** Plan de Recuperación de Desastres.
- **E20-2:** Plan para la Ampliación de Infraestructura de SISEM.
- **E20-3:** Manual de Operación y Mantenimiento de la Operación.
- **E20-4:** Mesa de Ayuda 7x24 (Niveles 1, 2 y 3) y ANS.
- **E20-5:** Aprovisionamiento, Despliegue y Configuración de Infraestructura de Nuevos Desarrollos.
- **E20-6:** Despliegue y Configuración de Infraestructura de Ambiente de Producción de Nuevos Desarrollos.

Este documento no reemplaza el detalle técnico de cada uno de los entregables, sino que presenta una **visión consolidada** de las actividades y logros alcanzados, enmarcando las acciones realizadas dentro de un contexto integral de gestión tecnológica. Asimismo, define las recomendaciones generales que permitirán al Fondo Financiero Distrital de Salud - Secretaría Distrital de Salud continuar con la administración, soporte y evolución del SISEM de acuerdo con las necesidades futuras.

### **3. Audiencia**

Este documento está dirigido a los usuarios técnicos del sistema y 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.

#### 4. Definiciones y Conceptos

|                                                                   |                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Actividades Generales Realizadas</b>                           | Conjunto de acciones desarrolladas durante la vigencia del contrato, orientadas al aprovisionamiento, despliegue y configuración de la infraestructura necesaria para garantizar la operación del Sistema de Emergencias Médicas (SISEM). Incluyen planeación técnica, esquemas de alta disponibilidad, seguridad, monitoreo, continuidad y soporte. |
| <b>Alta Disponibilidad</b>                                        | Diseño de infraestructura redundante que asegura la continuidad del servicio mediante replicación de bases de datos, despliegue en múltiples zonas de disponibilidad y balanceadores de carga que redistribuyen el tráfico ante fallos.                                                                                                              |
| <b>Automatización de Procesos</b>                                 | Implementación de scripts para estandarizar la instalación de software, actualización de dependencias, copias de seguridad y gestión de registros, con el fin de aumentar la eficiencia operativa y la confiabilidad.                                                                                                                                |
| <b>Gestión de Identidades y Accesos (IAM)</b>                     | Políticas y mecanismos de autenticación y autorización basadas en roles, utilizando herramientas como Keycloak para la emisión y validación de tokens de seguridad, asegurando trazabilidad y control de accesos.                                                                                                                                    |
| <b>Monitoreo y Observabilidad</b>                                 | Supervisión permanente de la infraestructura y servicios mediante métricas de CPU, memoria, red y almacenamiento, con alertamiento automático y centralización de registros para prevenir fallos y optimizar la operación.                                                                                                                           |
| <b>Seguridad y Hardening</b>                                      | Conjunto de prácticas de endurecimiento y protección de la infraestructura, incluyendo firewalls en múltiples niveles, certificados SSL, mitigación de ataques DDoS, uso de WAF y políticas de autenticación reforzada.                                                                                                                              |
| <b>Continuidad de Negocio y Recuperación ante Desastres (DRP)</b> | Estrategia integral para garantizar la disponibilidad del servicio ante contingencias, mediante replicación de datos en regiones espejo, respaldos automáticos, failover de servicios y pruebas periódicas de recuperación.                                                                                                                          |
| <b>Ambientes Tecnológicos (Dev, QA, Preprod, Prod)</b>            | Entornos diferenciados para el ciclo de vida del sistema: desarrollo (Dev), pruebas (QA), preproducción (Preprod) y producción (Prod), cada uno configurado con topologías y niveles de seguridad específicos.                                                                                                                                       |
| <b>Gestión de Incidentes, Problemas y Cambios</b>                 | Proceso estructurado de atención de eventos que afectan el servicio, incluyendo clasificación, análisis de causa raíz, resolución, escalamiento y control documentado de modificaciones en la infraestructura.                                                                                                                                       |
| <b>Mantenimiento Preventivo y Correctivo</b>                      | Actividades programadas y reactivas que aseguran el buen estado de la plataforma tecnológica, incluyendo aplicación de parches, actualización de software, ajustes de configuración y corrección de fallos.                                                                                                                                          |
| <b>Copias de Seguridad y Restauración de Datos</b>                | Política de respaldos periódicos de información y servicios críticos, con validación recurrente y planes de restauración para reducir tiempos de indisponibilidad en caso de fallos graves.                                                                                                                                                          |

|                            |                                                                                                                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mesa de Ayuda 7x24</b>  | Servicio de soporte técnico continuo dividido en niveles (1, 2 y 3), encargado de recibir, clasificar y atender incidentes y requerimientos bajo Acuerdos de Nivel de Servicio (ANS), asegurando la disponibilidad del sistema. |
| <b>Contenedores Docker</b> | Tecnología utilizada para empaquetar aplicaciones y servicios en entornos portables, optimizados y versionados, facilitando el despliegue en Kubernetes.                                                                        |
| <b>Kubernetes (GKE)</b>    | Plataforma de orquestación de contenedores utilizada en el SISEM para desplegar, administrar y escalar servicios en producción, complementada con Helm Charts y balanceadores de carga.                                         |
| <b>Keycloak</b>            | Gestor de identidad y autenticación implementado en el SISEM para administrar usuarios, roles, clientes y políticas de seguridad, garantizando control de accesos.                                                              |
| <b>Gestión de Logs</b>     | Centralización y análisis de registros de la infraestructura y servicios, habilitando trazabilidad de eventos, identificación de fallas y resolución eficiente de incidentes.                                                   |

## 5. Actividades Generales Realizadas

Durante la vigencia del contrato, se desarrollaron múltiples actividades orientadas al aprovisionamiento, despliegue y configuración de la infraestructura necesaria para garantizar el funcionamiento del Sistema de Emergencias Médicas (SISEM) en sus diferentes ambientes. Estas acciones abarcaron desde la planeación de la arquitectura técnica, la implementación de esquemas de alta disponibilidad, hasta la gestión integral de seguridad, monitoreo, continuidad y soporte de los entornos habilitados.

En primera instancia, se ejecutaron actividades de **conceptualización y diseño de alta disponibilidad**, enfocadas en asegurar la continuidad operacional del sistema. Esto incluyó la configuración redundante de bases de datos en Google Cloud SQL mediante instancias regionales con replicación síncrona, así como el despliegue de instancias de cómputo en diferentes zonas de disponibilidad, integradas con balanceadores de carga globales para redirigir tráfico en caso de fallos y mantener la disponibilidad del servicio. Igualmente, se implementaron mecanismos de escalado automático y reparación de instancias para responder a variaciones de demanda o fallas inesperadas.

De manera complementaria, se establecieron **scripts automatizados de inicio y apagado** en las máquinas virtuales, lo cual permitió estandarizar procesos de instalación de software, actualización de dependencias, generación de copias de seguridad y gestión de registros. Estos procedimientos contribuyeron a mejorar la eficiencia operativa y la confiabilidad del entorno.

En el frente de la **gestión de identidades y accesos**, se adoptaron políticas robustas de autenticación y autorización basadas en roles, utilizando mecanismos como Keycloak para la emisión y validación de tokens de seguridad. Se incluyó además la custodia de

accesos a la infraestructura en la nube, restringida al equipo de infraestructura y coordinadores responsables, asegurando la trazabilidad y el control sobre usuarios internos, contratistas y dispositivos externos.

La **administración y monitoreo** constituyó otra línea fundamental de actividades. Se configuraron herramientas de observabilidad en Google Cloud para todos los ambientes (desarrollo, pruebas, preproducción y producción), lo cual permitió recolectar métricas de CPU, memoria, red y almacenamiento a distintos niveles: infraestructura general, instancias de cómputo, APIs, bases de datos, Kubernetes (GKE), pods y contenedores. Estas métricas se complementaron con mecanismos de alertamiento automático, configurados para detectar umbrales críticos de uso de CPU y almacenamiento. Asimismo, se habilitaron registros (logs) centralizados y accesibles para el seguimiento detallado de eventos.

En cuanto a la **seguridad y hardening**, se implementaron múltiples capas de protección en la nube y en las bases de datos. Esto incluyó la definición de reglas de firewall en diferentes niveles (nodo, red VPC, pods de Kubernetes), el uso de certificados SSL para comunicaciones seguras vía HTTPS, la activación de servicios de mitigación contra ataques DDoS mediante Google Cloud Armor, así como la configuración de un WAF (Web Application Firewall) en el ambiente productivo. Adicionalmente, se establecieron estrategias de autenticación, control de accesos, copias de seguridad y resiliencia de datos para garantizar la confidencialidad e integridad de la información crítica del sistema.

En materia de **continuidad de negocio y recuperación ante desastres**, se dispusieron ambientes productivos en múltiples regiones de Google Cloud con esquemas de tolerancia a fallos. Esto se acompañó de la creación de réplicas de datos en una región espejo en Sudamérica, que puede ser activada en caso de contingencia. De igual manera, se implementaron respaldos para cargas de trabajo en Kubernetes, pods y bases de datos, junto con mecanismos de failover automático para garantizar la disponibilidad del servicio.

Finalmente, se realizó el **despliegue de los ambientes de desarrollo, pruebas (QA), preproducción y producción**, cada uno con su topología de red, instancias de cómputo y servicios configurados de acuerdo con las necesidades del proyecto. En el ambiente de desarrollo, se habilitaron múltiples máquinas virtuales y servicios de base de datos compartidos, con un enfoque en facilitar la labor de los equipos de desarrollo y pruebas. El ambiente de producción, por su parte, fue diseñado bajo un esquema de alta disponibilidad regional, con clusters distribuidos en varias zonas, IPs premium reservadas, reglas de seguridad específicas y servicios de balanceo de carga y firewall dedicados.

En conclusión, las actividades generales realizadas durante la vigencia del contrato comprendieron el diseño, aprovisionamiento, despliegue y aseguramiento integral de la

infraestructura tecnológica del SISEM, garantizando su operación continua, segura y escalable en los diferentes entornos definidos.

## **6. Operación y Mantenimiento**

Durante la vigencia del contrato, las actividades principales de operación y mantenimiento del Sistema de Emergencias Médicas (SISEM) estuvieron orientadas a garantizar la continuidad, estabilidad, seguridad y eficiencia de la plataforma tecnológica, en cumplimiento de los lineamientos definidos por la Secretaría Distrital de Salud. Estas actividades se pueden agrupar en varios ejes fundamentales:

### **1. Administración y monitoreo integral de la infraestructura tecnológica**

Se implementaron procedimientos de supervisión permanente sobre los distintos componentes del sistema, tales como servidores, bases de datos, balanceadores de carga, redes y contenedores. Este monitoreo permitió identificar comportamientos anómalos, prevenir caídas del servicio y asegurar que cada elemento funcionara dentro de los parámetros de capacidad y rendimiento esperados.

### **2. Gestión de incidentes, problemas y cambios**

Se estableció un proceso estructurado de atención de incidentes, que incluyó la recepción de reportes, análisis de la causa raíz, clasificación por niveles de prioridad y definición de tiempos de respuesta. En paralelo, se implementaron procedimientos de gestión de problemas recurrentes y de cambios en la infraestructura, garantizando que las modificaciones fueran documentadas, autorizadas y ejecutadas bajo control, minimizando el riesgo de afectación al servicio.

### **3. Mantenimiento preventivo y correctivo**

A lo largo de la operación se desarrollaron rutinas periódicas de verificación y ajuste en la plataforma. Estas incluyeron la actualización de software, aplicación de parches de seguridad, ajustes de configuración en servidores y bases de datos, así como la corrección de fallos detectados durante el monitoreo o reportados por los usuarios. El mantenimiento preventivo buscó anticipar problemas mediante revisiones programadas, mientras que el correctivo se orientó a solucionar fallas puntuales que impactaban el servicio.

### **4. Gestión de copias de seguridad y planes de contingencia**

Se implementó una política de respaldo periódico de la información y los servicios críticos. Las copias de seguridad se programaron y validaron de manera recurrente, garantizando que los datos pudieran ser recuperados en caso de fallas graves. Además, se definieron planes de contingencia y de recuperación ante desastres, los cuales incluyeron la activación de ambientes alternos y procedimientos de restauración para minimizar el tiempo de indisponibilidad del sistema.

#### **5. Monitoreo de seguridad y cumplimiento normativo**

Se ejecutaron controles de seguridad en diferentes niveles de la infraestructura. Esto comprendió la gestión de accesos y perfiles de usuarios, la aplicación de políticas de autenticación, la revisión de eventos sospechosos y la integración con herramientas de ciberseguridad como firewalls, WAF, antivirus y sistemas de detección de intrusiones. De igual manera, se aseguró el cumplimiento de lineamientos regulatorios y de buenas prácticas en la protección de la información sensible.

#### **6. Gestión de capacidad, disponibilidad y rendimiento**

Se realizaron evaluaciones periódicas del uso de recursos de cómputo, almacenamiento y red, ajustando la infraestructura para responder a las variaciones en la demanda. Esto permitió anticipar necesidades de escalabilidad, evitar saturaciones y mantener la disponibilidad de los servicios bajo condiciones de alta carga o eventualidades operativas.

#### **7. Soporte técnico y funcional a usuarios y equipos relacionados**

Se prestó atención constante a los requerimientos de los diferentes actores involucrados en la operación del SISEM. El soporte incluyó la resolución de dudas, la atención a fallas reportadas, la asistencia en la ejecución de pruebas y la guía en el uso de los servicios, garantizando la satisfacción y confianza de los usuarios en la estabilidad del sistema.

#### **8. Documentación, reportes y trazabilidad**

Como parte de la operación, se elaboraron informes periódicos, manuales técnicos, guías de procedimientos y actas de seguimiento, los cuales documentaron de manera formal las actividades realizadas, los incidentes atendidos y las evidencias de las acciones ejecutadas. Esto aseguró trazabilidad en la gestión, permitió el seguimiento contractual y facilitó la transferencia de conocimiento para la continuidad del servicio.

### **7. Recuperación de Desastres**

El **Plan de Recuperación de Desastres (DRP)** elaborado para el sistema SISEM constituye una pieza fundamental dentro de las actividades de soporte, mantenimiento y operación. Su propósito fue establecer una estrategia integral que asegurara la **continuidad operativa** de la plataforma, la protección de la información y la capacidad de reacción frente a escenarios de indisponibilidad total.

Las actividades principales desarrolladas en el marco de este plan se concentraron en los siguientes aspectos:

1. **Análisis de riesgos y escenarios críticos**

Se llevó a cabo la identificación de riesgos potenciales que pudieran afectar la operación del sistema, incluyendo causas de origen natural (inundaciones, incendios, pandemias), humano (errores de operación, sabotajes, ciberataques) y técnico (fallas de hardware, interrupciones de red, caídas de servicios en la nube). A partir de este análisis se definió el escenario crítico de **falla total de la plataforma en la zona primaria de Google Cloud**, el cual constituye la base del **DRP**.

2. **Definición de tiempos de recuperación (RPO, RTO, WRT y MTD)**

Se establecieron los parámetros que delimitan la capacidad de respuesta:

- **RPO (Recovery Point Objective):** 4 horas como pérdida máxima aceptable de datos.
- **RTO (Recovery Time Objective):** 2 horas para restablecer la operación de la plataforma.
- **WRT (Work Recovery Time):** 1 hora para validación y verificación de integridad.
- **MTD (Maximum Tolerable Downtime):** 3 horas como máximo de interrupción aceptable.

Estos indicadores permiten alinear las expectativas operativas con las capacidades de recuperación del sistema.

3. **Diseño e implementación de la estrategia de recuperación**

El plan contempló la configuración de la plataforma bajo un esquema de **alta disponibilidad**, distribuyendo los recursos en múltiples zonas de Google Cloud (us-east1-b y us-east1-c). Se desplegaron cinco nodos redundantes que permiten la **conmutación automática** hacia regiones alternas en caso de una falla en la zona primaria, alcanzando así una disponibilidad del **99.99%**.

4. **Gestión de respaldos y restauración de datos**

Se implementaron mecanismos de copia de seguridad diaria del clúster completo, con retención de siete días, garantizando que en caso de desastre la restauración pueda realizarse utilizando la copia más reciente, preservando la integridad de los datos y reduciendo al mínimo la pérdida de información crítica.

5. **Simulación y pruebas de recuperación**

Se definió la realización de ejercicios anuales de replicación y simulación del escenario de falla total. Estas prácticas permiten no solo validar la efectividad del plan, sino también fortalecer la preparación del equipo técnico ante emergencias

reales, identificar oportunidades de mejora y mantener actualizado el protocolo de actuación.

#### 6. **Roles, responsabilidades y comunicación en situaciones de desastre**

Se documentó un esquema claro de responsabilidades:

- **Mesa de Ayuda:** primera línea de recepción de incidencias y monitoreo.
- **Coordinador de Recuperación (Director de TI):** responsable de declarar el desastre, activar el plan y liderar la estrategia.
- **Equipo de Infraestructura:** encargado de restaurar servidores, sistemas operativos y conectividad.
- **Equipo de Aplicaciones y Desarrollo:** responsable de la recuperación y validación de software y datos.
- **Gerente de Proyecto:** garante de la comunicación permanente con la Secretaría Distrital de Salud y de la articulación con los equipos de ETB. Este modelo asegura un **flujo de comunicación estructurado**, tanto interno como externo, reduciendo tiempos de respuesta y garantizando transparencia frente a los actores involucrados.

#### 7. **Retorno a la normalidad y automatización**

Se configuró el **aprovisionamiento automático de nodos**, que permite escalar o restablecer la infraestructura sin intervención manual, así como la generación de **alertas y logs automáticos** sobre el uso de recursos y eventos críticos, supervisados por la mesa de servicios. Este enfoque permite que la transición entre zonas afectadas y operativas sea transparente para el usuario final.

#### 8. **Conclusiones del plan**

La implementación del DRP consolidó un esquema de **resiliencia tecnológica** que no depende de acciones manuales para su activación, reforzando la capacidad del SISEM de garantizar la prestación continua de servicios esenciales aun en condiciones de interrupciones graves. Asimismo, fortaleció la coordinación entre los equipos técnicos, administrativos y de gestión, generando un marco confiable para la protección de los intereses institucionales.

### 8. **Mesa de Ayuda 7x24 (Nivel 1, 2 y 3) y ANS**

En el marco del contrato, se estableció la **Mesa de Ayuda 7x24** como un componente estratégico para garantizar la atención continua de incidentes, requerimientos y problemas relacionados con la operación del SISEM. Este servicio se implementó bajo un modelo escalonado de soporte (niveles 1, 2 y 3) y bajo el cumplimiento de **Acuerdos de Nivel de Servicio (ANS)** definidos contractualmente, con el fin de asegurar la disponibilidad y continuidad del sistema.

Las actividades principales desarrolladas en el marco de este componente fueron:

#### 1. **Atención y gestión integral de incidentes**

- Se garantizó la recepción, registro y clasificación de todos los incidentes reportados a través de la Mesa de Ayuda.

- Los incidentes fueron priorizados con base en su impacto y urgencia, asignando tiempos de respuesta y resolución conforme a los ANS.
  - Se implementaron mecanismos de seguimiento y escalamiento oportuno hacia niveles superiores de soporte, reduciendo los tiempos de indisponibilidad.
2. **Soporte por niveles (1, 2 y 3)**
- **Nivel 1:** atención inicial, registro en la herramienta de gestión, resolución de casos básicos y canalización de solicitudes.
  - **Nivel 2:** análisis especializado para incidentes recurrentes o de mayor complejidad, aplicando procedimientos correctivos y preventivos.
  - **Nivel 3:** soporte avanzado a nivel de infraestructura y desarrollo, abordando problemas críticos relacionados con la plataforma en la nube, bases de datos y aplicaciones del SISEM.
3. **Gestión de requerimientos y solicitudes de servicio**
- La Mesa de Ayuda procesó solicitudes de carácter operativo y técnico (como creación de usuarios, accesos, despliegue de servicios o ajustes de configuración).
  - Se implementaron procedimientos estandarizados para garantizar trazabilidad, desde la solicitud inicial hasta su cierre.
4. **Monitoreo y reportes de cumplimiento (ANS)**
- Se establecieron indicadores de desempeño asociados a tiempos de respuesta, resolución y satisfacción del usuario.
  - Los reportes periódicos permitieron verificar el cumplimiento de los compromisos contractuales y evidenciar el nivel de servicio entregado.
  - Se documentaron las métricas de disponibilidad y continuidad, así como los casos en los que fue necesario activar mecanismos de escalamiento.
5. **Soporte proactivo y preventivo**
- Además de la atención reactiva, se desarrollaron actividades preventivas orientadas a anticipar fallas, como revisiones periódicas de registros, identificación de patrones de incidentes y análisis de tendencias.
  - Se promovió la retroalimentación hacia los equipos de infraestructura y desarrollo para implementar mejoras continuas en la plataforma.
6. **Gestión de la comunicación y satisfacción del usuario**
- Se mantuvo un canal constante de comunicación con los diferentes actores del SISEM, garantizando información clara sobre el estado de los incidentes y requerimientos.
  - Se midió la satisfacción de los usuarios respecto a los tiempos y calidad de las respuestas, utilizando esta retroalimentación para fortalecer la atención.
7. **Soporte continuo 7x24**
- Se aseguró la disponibilidad de personal y recursos técnicos durante las 24 horas del día, los 7 días de la semana, incluyendo días festivos.
  - Este modelo permitió responder oportunamente a incidentes críticos que pudieran ocurrir fuera del horario laboral, evitando afectaciones graves en la operación del sistema.

Se anexan los informes correspondientes de la Mesa de Servicio y del consumo de infraestructura, los cuales se encuentran disponibles para su consulta en el repositorio compartido.

[https://drive.google.com/drive/folders/1H5v6A4nLU6QFxoVXj3P81aoLflHp65L?usp=drive\\_link](https://drive.google.com/drive/folders/1H5v6A4nLU6QFxoVXj3P81aoLflHp65L?usp=drive_link)

## **9. Aprovisionamiento, Despliegue y Configuración de Infraestructura de Nuevos Desarrollos**

El componente de **aprovisionamiento, despliegue y configuración de la infraestructura** tuvo como objetivo principal garantizar que el SISEM contara con entornos tecnológicos robustos, seguros y escalables para soportar tanto la operación actual como los nuevos desarrollos requeridos por la Secretaría Distrital de Salud. Este entregable estuvo enfocado en la construcción de ambientes estandarizados y en la aplicación de buenas prácticas de arquitectura en la nube, buscando asegurar la continuidad del servicio y la capacidad de adaptación a futuros requerimientos.

Las actividades principales ejecutadas en este marco fueron las siguientes:

### **1. Diseño de esquemas de alta disponibilidad y redundancia**

- Se configuraron instancias de bases de datos en Google Cloud SQL bajo un modelo regional con replicación síncrona para garantizar la resiliencia.
- Se desplegaron instancias de cómputo en múltiples zonas de disponibilidad, integradas con balanceadores de carga globales que permiten redistribuir el tráfico en caso de fallos.
- Se habilitaron mecanismos de escalado automático (autoscaling) y reparación automática de instancias para responder a picos de demanda y mantener la estabilidad de los servicios.

### **2. Automatización de procesos de despliegue y mantenimiento**

- Se desarrollaron scripts que permiten la automatización del aprovisionamiento de máquinas virtuales, instalación de dependencias, actualizaciones y copias de seguridad.
- Estas rutinas garantizan la estandarización en la configuración de los ambientes y reducen los tiempos de despliegue, aumentando la eficiencia operativa.

### **3. Gestión de identidades y accesos**

- Se implementaron políticas de autenticación y autorización basadas en roles (RBAC), utilizando Keycloak como mecanismo de validación de tokens de seguridad.
- Se aplicaron controles estrictos de acceso a la infraestructura en la nube, con trazabilidad de acciones y segregación de funciones entre usuarios, contratistas y administradores.

### **4. Monitoreo y observabilidad de la infraestructura**

- Se habilitaron paneles de control con métricas de CPU, memoria, red y almacenamiento en Google Cloud Monitoring.
  - El monitoreo abarcó diferentes niveles de detalle: infraestructura general, instancias de cómputo, APIs, bases de datos, clústeres de Kubernetes, pods y contenedores.
  - Se configuraron alertas automáticas ante umbrales críticos de uso de recursos, así como la centralización de logs para análisis y auditoría.
5. **Seguridad y hardening de la plataforma**
- Se configuraron reglas de firewall en distintos niveles (nodos, redes VPC y pods de Kubernetes).
  - Se implementaron certificados SSL para la comunicación segura mediante HTTPS.
  - Se integraron servicios de mitigación contra ataques DDoS mediante Google Cloud Armor, junto con la activación de un Web Application Firewall (WAF) en el ambiente productivo.
  - Se aplicaron prácticas de endurecimiento de servidores y bases de datos para proteger la confidencialidad e integridad de la información.
6. **Continuidad de negocio y recuperación ante fallos**
- Se desplegaron ambientes de producción con distribución regional en varias zonas de Google Cloud, asegurando tolerancia a fallos.
  - Se estableció una región espejo en Sudamérica para replicar datos y habilitar la activación en caso de contingencia.
  - Se implementaron mecanismos de failover automático para minimizar la indisponibilidad del servicio.
7. **Despliegue de ambientes de desarrollo, pruebas, preproducción y producción**
- Se crearon ambientes diferenciados, cada uno con su propia topología de red y configuraciones específicas:
    - **Desarrollo:** con múltiples máquinas virtuales y bases de datos compartidas para facilitar la labor de los equipos técnicos.
    - **Pruebas (QA):** con servicios replicados para simular condiciones de producción.
    - **Preproducción:** como entorno de validación previa antes de la puesta en marcha final.
    - **Producción:** diseñado bajo criterios de alta disponibilidad, seguridad reforzada y balanceo de carga para garantizar la continuidad del servicio.

## 10. Despliegue y Configuración de Infraestructura de Ambiente de Producción de Nuevos Desarrollos

El presente entregable tuvo como propósito establecer las directrices y procedimientos para la **puesta en producción del SISEM**, asegurando que los nuevos desarrollos se desplegaran en un entorno controlado, seguro y altamente disponible. Este documento sirvió como manual operativo para los equipos técnicos, detallando cada uno de los

procesos necesarios para garantizar una migración exitosa desde entornos de desarrollo y pruebas hacia la infraestructura definitiva de producción.

Las principales actividades realizadas fueron:

#### 1. **Generación de contenedores**

- Se implementó una metodología basada en **imágenes Docker**, optimizada para reducir el tamaño de los contenedores y mejorar los tiempos de despliegue.
- El proceso incluyó la compilación de proyectos desarrollados en **TypeScript a JavaScript**, ejecutada en dos fases: una con dependencias de desarrollo y otra con dependencias estrictamente de producción.
- Para los servicios frontend en Angular se utilizó una imagen base de **Nginx**, garantizando un rendimiento adecuado en la entrega de contenido estático.
- Se estableció un esquema de **etiquetado de imágenes por versiones**, lo que permite trazabilidad y control de las implementaciones.

#### 2. **Despliegue del producto en Kubernetes**

- Inicialmente el sistema fue desplegado mediante Docker Compose; sin embargo, el entorno productivo adoptó **Kubernetes (GKE en Google Cloud Platform)** como plataforma de orquestación.
- Se configuraron **charts de Helm** para centralizar la administración de variables, imágenes, secretos, dominios y credenciales, facilitando la estandarización del despliegue.
- Se habilitaron balanceadores de carga, certificados de seguridad con **Cert Manager** y configuración de dominios personalizados.
- Aunque no se aplicó escalado automático en esta fase, se dejó preparado el entorno para su habilitación futura, en función de métricas operativas reales.

#### 3. **Instalación y configuración del Realm de Keycloak**

- Se desplegó el servicio de **Keycloak** como gestor de identidad y autenticación, configurando realms, clientes, roles, grupos y mapeos de seguridad.
- Se automatizó la instalación inicial mediante un **script especializado**, evitando la necesidad de configuraciones manuales recurrentes.
- Este procedimiento aseguró un modelo de seguridad robusto y replicable en todos los entornos.

#### 4. **Conexión a bases de datos**

- Las bases de datos fueron aisladas dentro del clúster de Kubernetes, sin accesos públicos directos, reforzando la seguridad.
- Para la gestión de datos, se definió un esquema de conexión mediante **túneles seguros (kubectrl port-forward)**, garantizando que solo personal autorizado pudiera acceder con credenciales controladas.
- Este enfoque aseguró el equilibrio entre **protección de la información** y la **operatividad de los equipos técnicos** para tareas de soporte y mantenimiento.

**5. Gestión y visualización de logs**

- Se configuró la centralización de registros utilizando las facilidades de Google Cloud Platform, permitiendo revisar los logs de cada pod directamente desde la consola.
- Esto facilitó la identificación de fallas, la trazabilidad de procesos y el análisis de incidentes en tiempo real, optimizando los tiempos de resolución.

**6. Servicio de notificaciones**

- Se implementó un servicio dedicado para la gestión de notificaciones, habilitado para recibir archivos de entrada con credenciales de integración hacia proveedores externos.
- El servicio contempló la administración de **plantillas de correo electrónico y mensajes**, asegurando la personalización y estandarización de las comunicaciones del sistema.

**11. Documentos entregados Entregable E20 – Infraestructura, Soporte, Mantenimiento y Operación 2023.**

En cumplimiento de lo establecido contractualmente, se informa que **ETB S.A. E.S.P ha publicado en el repositorio compartido los documentos correspondientes al entregable**, los cuales respaldan y evidencian el desarrollo de las actividades realizadas. Dichos documentos atienden de manera específica las obligaciones pactadas en el contrato y permiten verificar el cumplimiento de los compromisos adquiridos. A continuación, se relacionan los documentos entregados:

[https://drive.google.com/drive/folders/1LOlkPwXHEuAqzoxfSeFk5WRoWOSwmqns?usp=drive\\_link](https://drive.google.com/drive/folders/1LOlkPwXHEuAqzoxfSeFk5WRoWOSwmqns?usp=drive_link)

Contenido:

| <b>Documento del contrato</b>                       | <b>Entregable</b>                                                     |
|-----------------------------------------------------|-----------------------------------------------------------------------|
| Mesa de ayuda 7X24 (Nivel 1, 2 y 3)                 | SISEM-3-E20-4 Mesa de Ayuda 7X24 (Nivel 1, 2 y 3) y ANS.pdf           |
| Manual de operación y mantenimiento de la operación | SISEM-2-E20-3 Manual de Operación y Mantenimiento de la Operación.pdf |
| Presentación de modelo de ANS                       | SISEM-3-E20-4 Mesa de Ayuda 7X24 (Nivel 1, 2 y 3) y ANS.pdf           |
| Ejecución de Soporte y Mantenimiento de Solución    | Informes mesa de ayuda e infraestructura                              |
| Informe Mensual                                     | Informes mesa de ayuda e infraestructura                              |

| Documento del contrato                                                                                                                                          | Entregable                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informes mensuales de gestión de operación.                                                                                                                     | Informes mesa de ayuda e infraestructura                                                                                                                                            |
| Despliegue y configuración de infraestructura de ambiente de producción de nuevos desarrollos                                                                   | SISEM-3-E20-6 Despliegue y configuración de infraestructura de ambiente de producción.pdf SISEM-3-E20-6 Despliegue y configuración de infraestructura de ambiente de producción.pdf |
| Aprovisionamiento, despliegue y configuración de infraestructura de nuevos desarrollos en los ambientes QA, Desarrollo, producción para los nuevos desarrollos. | SISEM-3-E20-5 Aprovisionamiento, Despliegue y Configuración de Infraestructura de Nuevos Desarrollos.pdf                                                                            |
| Monitoreo y gestión de Infraestructura                                                                                                                          | Informes mesa de ayuda e infraestructura                                                                                                                                            |

| Nombre                                                                                                   | Última modificación | Tamaño del í |  |
|----------------------------------------------------------------------------------------------------------|---------------------|--------------|--|
| V2                                                                                                       | 5 ago 2025 yo       | —            |  |
| SISEM-2-E20-3 Manual de Operación y Mantenimiento de la Operación.pdf                                    | 23 nov 2023 yo      | 2 MB         |  |
| SISEM-3-E20-1 Plan de Recuperación de Desastres.pdf                                                      | 23 nov 2023 yo      | 509 KB       |  |
| SISEM-3-E20-2 Plan Para la Ampliación de Infraestructura de SISEM.pdf                                    | 23 nov 2023 yo      | 384 KB       |  |
| SISEM-3-E20-4 Mesa de Ayuda 7X24 (Nivel 1, 2 y 3) y ANS.pdf                                              | 23 nov 2023 yo      | 468 KB       |  |
| SISEM-3-E20-5 Aprovisionamiento, Despliegue y Configuración de Infraestructura de Nuevos Desarrollos.pdf | 23 nov 2023 yo      | 3.9 MB       |  |
| SISEM-3-E20-6 Despliegue y configuración de infraestructura de ambiente de producción.pdf                | 23 nov 2023 yo      | 555 KB       |  |

*Ilustración 1. Documentos entregable E20*

| Nombre                                                                                                   | Última modificación | Tamaño del í |  |
|----------------------------------------------------------------------------------------------------------|---------------------|--------------|--|
| SISEM-3-E20-5 Aprovisionamiento, Despliegue y Configuración de Infraestructura de Nuevos Desarrollos.pdf | 23 sept 2024 yo     | 3.9 MB       |  |
| SISEM-3-E20-6 Despliegue y configuración de infraestructura de ambiente de producción.pdf                | 23 sept 2024 yo     | 563 KB       |  |

*Ilustración 2. Documentos Entregable E20, carpeta V2*

## 12. Recomendaciones para la Administración y Soporte de la Infraestructura

### Definir un Administrador de Plataforma GCP

ETB recomienda a la SDS designar formalmente un administrador responsable de la plataforma de Google Cloud Platform (GCP), quien deberá gestionar las configuraciones, accesos,

contraseñas y demás parámetros de seguridad. Este rol debe tener trazabilidad de cambios y control sobre la delegación de permisos a otros usuarios o contratistas.

### **Validar Costos Asociados a la Salida a Producción**

Previo a la puesta en producción, la SDS debe realizar un análisis detallado de los costos asociados a los servicios que se habiliten en la nube, incluyendo elementos como dominios institucionales (.gov.co), consumo de cómputo, almacenamiento, balanceadores de carga y servicios de seguridad GCP. Esto permitirá asegurar la sostenibilidad financiera de la operación.

### **Establecer Políticas de Seguridad y Gestión de Accesos**

La SDS debe adoptar políticas de seguridad basadas en roles (RBAC), definiendo perfiles diferenciados para administradores, desarrolladores, contratistas y usuarios. Es fundamental mantener controles de autenticación robustos (ej. MFA) y rotación periódica de credenciales.

### **Implementar un Esquema de Monitoreo y Alertamiento**

Se recomienda habilitar paneles de monitoreo en GCP para observar métricas de CPU, memoria, almacenamiento, red, servicios de Kubernetes y bases de datos. Asimismo, se deben configurar alertas automáticas para detectar anomalías de rendimiento, sobrecarga o intentos de intrusión.

### **Plan de Continuidad y Recuperación ante Desastres (DRP)**

La SDS debe mantener activo el esquema de respaldos automáticos y replicación en región espejo, validando periódicamente los procedimientos de restauración y failover. También es recomendable realizar simulacros anuales de contingencia para fortalecer la preparación del equipo técnico.

### **Gestionar la Capacidad y Escalabilidad**

La entidad debe realizar evaluaciones periódicas del consumo de recursos para anticipar necesidades de ampliación de cómputo, almacenamiento o red, ajustando la infraestructura de acuerdo con la demanda.

### **Consolidar la Documentación Técnica y Operativa**

Se recomienda centralizar en un repositorio único la documentación de configuraciones, manuales, guías de operación y credenciales institucionales, asegurando su actualización constante y el acceso exclusivo de los responsables autorizados.

**Fin del Documento**