Acreditada en Alta Calidad
Res. nº. 29499 del Mineducación. 29/12/17 vigencia 28/12/21

FACULTAD DE INGENIERÍA

PROYECTO DE INTEGRACIÓN

PROYECTO SIMAI (SISTEMA INTEGRADO DE MONITOREO Y ANÁLISIS DE INCIDENTES)

ESTUDIANTE LUIS FELIPE ARIAS CARRIAZO

PROGRAMA ACADÉMICO INGENIERÍA DE SISTEMAS - VIRTUAL

MONITOR ACADÉMICO

JOHN JAIRO PORRAS

BOGOTÁ D.C.

25/05/2025

TABLA DE CONTENIDO

Resumen Ejecutivo 7

Introducción 8

Objetivos del proyecto 12

Objetivo General 12

Objetivos Específicos 12

Definición del problema 13

Justificación 16

Análisis de Requerimientos 18

Intención del Producto 18

Herramientas y Servicios para el Diseño Arquitectónico 18

Requerimientos Funcionales para el Diseño Arquitectónico 19

Centralización de Monitoreo 19

Componentes Azure por Especificar: 19

Origen y destino de datos en la arquitectura SIMAI 20

Gestión de Alertas e Incidentes (Diseño Conceptual) 20

Componentes Azure por especificar: 21

Análisis de Datos y Correlación (Diseño Conceptual) 21

Componentes Azure Por Especificar: 22

Reportes y Dashboards (Diseño Conceptual) 22

Componentes Azure por especificar: 23

Gestión de Usuarios y Roles (Diseño Conceptual) 23
Componentes Azure por Especificar: 23
Requerimientos No Funcionales para el Diseño Arquitectónico 25
Marco Teórico 27
Benchmarking y soluciones similares: 29
Análisis de restricciones 31
Restricciones Ambientales 31
Restricciones Económicas 33
Restricciones Legales 34
Restricciones de Salud y Seguridad 35
Restricciones Socioculturales 36
Restricciones Técnicas Adicionales 37
Metodología para la selección y desarrollo de la solución 39
Criterios de selección metodológica 39
Azure Well-Architected Framework 40
The Twelve-Factor App 40
TOGAF + Cloud Adaptations 41
Instrumentos de recolección de información 43
Análisis de costos 44
Clasificación General de Costos en el Proyecto SIMAI 44
Costos Directos 44

Recursos de infraestructura en Azure 44
Licencias y herramientas externas 45
Costos Indirectos 46
Capital de Trabajo 47
Recursos humanos 47
Insumos operativos 47
Consideraciones adicionales 48
Diseño de la Arquitectura de Software 50
Descripción General 50
Explicación del Diagrama de Arquitectura 51
Fuentes de Datos y Monitoreo 51
Plataforma Centralizada en Azure 51
Procesamiento y Almacenamiento 51
Seguridad y Acceso 52
Visualización y Exploración 52
Flujo de Datos y Procesos 53
Justificación de la Arquitectura 54
Conclusiones 55
Aspectos novedosos desarrollados 56
Referencias 57

INDICE DE TABLA

Tabla 1. Descripción de orígenes de datos arquitectura SIMAI. Fuente: Diseño Propio . 20

Tabla 2: Historias de Usuario. Fuente: Diseño propio 26

Tabla 3. Trazabilidad de Requerimientos. Fuente: Diseño propio. 26

Tabla 4: Descripción de restricciones ambientales. Fuente: Diseño propio 32

Tabla 5: Descripción de restricciones económicas. Fuente: Diseño propio. 34

Tabla 6: Descripción de restricciones Legales. Fuente: Diseño propio 35

Tabla 7: Descripción de restricciones de salud y seguridad. Fuente: Diseño propio. 36

Tabla 8: Descripción de restricciones socioculturales. Fuente: Diseño propio. 37

Tabla 9: Descripción de restricciones Tecnicas. Fuente: Diseño propio. 38

Tabla 10: Metodología. Fuente: Diseño propio 42

Tabla 11: Marcos Metodológicos - Comparación. Fuente: Diseño propio 43

Tabla 12: Estimación de Costos - Mes a Mes. Fuente: Diseño propio. 45

Tabla 13: Costo de licenciamiento. Fuente: Diseño propio 46

Tabla 14: Estimación salarios -Mes. (tres meses). Fuente: Diseño Propio. 47

Tabla 15: Estimación Global. Fuente: Diseño propio. 48

Tabla 16: Descripción de soluciones comerciales. Fuente: Diseño propio 48

TABLA DE ILUSTRACIONES

Ilustración 1: Propuesta de diseño de arquitectura. Fuente: Diseño propio..... 50

Resumen Ejecutivo

En la actualidad, las organizaciones dependen de sistemas tecnológicos avanzados para garantizar la continuidad de sus operaciones. Sin embargo, los métodos tradicionales de monitoreo presentan diversas limitaciones, como la falta de integración entre plataformas, la gestión manual de incidentes y la dificultad para correlacionar eventos en tiempo real. Esto genera retrasos en la identificación y resolución de problemas, afectando la disponibilidad y seguridad de los servicios.

El Sistema Integrado de Monitoreo y Análisis de Incidentes (SIMAI) surge como una solución para abordar estas problemáticas mediante el diseño de una arquitectura optimizada basada en Microsoft Azure. Su objetivo es centralizar el monitoreo, mejorar la detección y análisis de incidentes y reducir la dependencia de la intervención manual, garantizando eficiencia en la toma de decisiones y cumplimiento de los marcos de referencia ITIL.

Con este enfoque, SIMAI busca proporcionar una solución escalable y segura, capaz de optimizar la gestión de incidentes en entornos empresariales, mejorando la eficiencia operativa y reduciendo tiempos de respuesta ante incidentes críticos.

Introducción

El desarrollo del proyecto SIMAI se fundamenta en la necesidad crítica de las organizaciones modernas, como Global Hitss, de contar con soluciones que permitan gestionar proactivamente su infraestructura tecnológica a través de una arquitectura de monitoreo centralizada y automatizada. En un entorno altamente competitivo y digitalizado, donde los servicios TI son el núcleo de operación empresarial, cualquier retraso en la identificación y análisis de incidentes representa una amenaza directa para la continuidad del negocio y el cumplimiento de acuerdos de nivel de servicio (SLA).

Global Hitss, como proveedor de servicios gestionados de TI, opera una infraestructura distribuida que da soporte a entidades del sector financiero, telecomunicaciones, retail, entre otros. La multiplicidad de herramientas actualmente en uso (Zabbix, Dynatrace, Grafana, Kibana) genera silos de información y dificulta la correlación de eventos, lo cual impacta directamente en la eficiencia operativa. En este contexto, el diseño de una arquitectura técnica unificada no solo es pertinente, sino también estratégico para alinear los procesos de monitoreo con las buenas prácticas del sector.

Adicionalmente, la operación de Global Hitss abarca la gestión de grandes volúmenes de datos, eventos y métricas provenientes de distintas fuentes, lo que incrementa la complejidad en la administración y la respuesta ante incidentes. La falta de integración y automatización en el monitoreo puede derivar en la duplicidad de esfuerzos, errores humanos y pérdida de trazabilidad, factores que afectan la calidad del servicio y la satisfacción del cliente.

Es necesario destacar que ITIL v4 (Information Technology Infrastructure Library) actúa como un marco de referencia, el cual proporciona lineamientos estructurados para la gestión de servicios TI con un enfoque en la mejora continua, la entrega de valor y la alineación entre TI y

el negocio (Axelos, 2019). En este proyecto, ITIL v4 guía el diseño de los componentes arquitectónicos en aspectos como la gestión de incidentes, gestión de eventos, disponibilidad y cumplimiento.

La integración de herramientas especializadas en monitoreo y análisis, como Zabbix, Dynatrace, Grafana, Kibana y Elasticsearch, es fundamental para lograr una visión unificada y centralizada de la operación tecnológica. Cada una de estas plataformas aporta capacidades específicas: Zabbix permite el monitoreo detallado de infraestructura, Dynatrace habilita el análisis avanzado de aplicaciones y servicios con inteligencia artificial, Grafana y Kibana ofrecen visualización avanzada de métricas y logs, y Elasticsearch proporciona almacenamiento y búsqueda eficiente de grandes volúmenes de datos.

Desde la perspectiva académica, el diseño arquitectónico de SIMAI representa una aplicación avanzada de principios de ingeniería de sistemas, orientados a la estructuración de soluciones escalables, resilientes y orientadas al cumplimiento normativo. A diferencia de un proyecto de desarrollo, el alcance de SIMAI se limita al diseño conceptual de la arquitectura, lo cual implica definir flujos de datos, estructuras de integración, selección de componentes y alineación con marcos regulatorios, sin comprometerse con la implementación funcional.

Para justificar técnicamente la elección de herramientas, se hace necesario destacar sus características clave dentro del diseño:

Zabbix: herramienta open-source especializada en monitoreo de red e infraestructura. Su capacidad para generar alertas personalizadas y recolectar métricas de dispositivos físicos y virtuales, permite establecer nodos de recolección dentro de la arquitectura propuesta (Zabbix, 2023). La arquitectura considera su integración como origen de eventos, preservando la inversión existente de Global Hitss.

Grafana: permite la visualización de datos en tiempo real, soportando múltiples fuentes como Prometheus, Elasticsearch o bases SQL. En la arquitectura de SIMAI, Grafana se ubica como componente visual para la exposición de dashboards a nivel operativo (Grafana Labs, 2023).

Kibana: herramienta gráfica del stack ELK, cuya función principal es la visualización avanzada de logs estructurados. En la propuesta arquitectónica, Kibana se posiciona como componente de análisis para equipos de N1 y N2, facilitando el diagnóstico y trazabilidad de eventos (Elastic, 2023).

Elasticsearch: se considera dentro del diseño como núcleo para la indexación y búsqueda rápida de eventos en grandes volúmenes. Su integración es vital para establecer una base de datos de observabilidad, desde donde los componentes analíticos extraen información para correlación (Gormley & Tong, 2015).

Dynatrace: en el diseño se concibe como el motor de análisis APM (Application Performance Monitoring) orientado al rendimiento y trazabilidad de servicios. Su componente de inteligencia artificial, Davis AI, permite correlacionar causas raíz en entornos complejos, lo que complementa el diseño orientado a eventos críticos (Dynatrace, 2023).

El diseño arquitectónico de SIMAI, además, contempla la interoperabilidad de estas herramientas con los servicios nativos de Azure, como Azure Monitor, Log Analytics, Event Hub y Logic Apps, para lograr la centralización, correlación y visualización eficiente de la información crítica. La arquitectura propuesta permite que los datos generados por cada plataforma se integren y procesen en la nube, facilitando la automatización de alertas, la generación de reportes y dashboards unificados, y la trazabilidad de la operación.

Todas estas herramientas fueron seleccionadas considerando su compatibilidad con entornos en la nube como Microsoft Azure y su capacidad de interoperabilidad. El diseño arquitectónico de SIMAI incluye una propuesta de integración lógica entre estas plataformas mediante flujos de datos centralizados, orquestados a través de servicios como Azure Monitor, Event Hub y Logic Apps.

Además, se ha tomado en cuenta la estrategia de seguridad de la información, basando el diseño en estándares internacionales como ISO/IEC 27001:2013, el cual ya se encuentra implementado en Global Hitss. Esto refuerza la necesidad de que la arquitectura incorpore mecanismos de control de acceso, cifrado, trazabilidad de acciones (logs de auditoría) y gestión de identidades con Azure Active Directory y roles RBAC.

Desde el punto de vista de sostenibilidad tecnológica, SIMAI también se justifica como una solución que preserva inversiones previas, reduce el costo total de propiedad (TCO) y disminuye el esfuerzo humano repetitivo, alineando a Global Hitss con la transformación digital y la operación basada en datos. A mediano plazo, este diseño puede servir como base para futuras implementaciones funcionales, pero actualmente cumple el rol de establecer los cimientos de una solución técnica escalable y modular.

En síntesis, la introducción de este proyecto no solo contextualiza la problemática y la necesidad de una solución integral, sino que también justifica la selección de herramientas, la alineación con marcos internacionales y la pertinencia académica y profesional del diseño arquitectónico propuesto, asegurando que SIMAI sea una respuesta robusta y sostenible a los retos actuales y futuros de la gestión de monitoreo en Global Hitss Colombia.

Objetivos del proyecto

Objetivo General

Desarrollar el diseño de la arquitectura para la implementación de un sistema de monitoreo basado en Azure, asegurando escalabilidad, seguridad y cumplimiento de marcos ITIL.

Objetivos Específicos

- Definir los requerimientos funcionales y no funcionales del sistema.
- Diseñar la arquitectura utilizando servicios de Azure.
- Evaluar la viabilidad del diseño en términos de costos y capacidades técnicas.
- Asegurar que la arquitectura cumpla con los marcos de referencia ITIL.

Definición del problema

En el contexto de Global Hitss, una empresa líder en servicios de outsourcing y soluciones tecnológicas se ha identificado una problemática recurrente relacionada con la dispersión de herramientas de monitoreo y la ausencia de una arquitectura unificada para la gestión centralizada de eventos, métricas y análisis de rendimiento. La organización brinda soporte a diversos sectores estratégicos como banca, telecomunicaciones y servicios públicos, lo cual implica altos niveles de exigencia en términos de disponibilidad, trazabilidad y cumplimiento de Acuerdos de Nivel de Servicio (SLA).

Actualmente, el equipo de monitoreo de Global Hitss opera mediante múltiples plataformas como Zabbix, Dynatrace, Grafana y Kibana, lo cual, si bien permite una observabilidad amplia, genera silos de información y procesos manuales de correlación de eventos que ralentizan la toma de decisiones. Esta fragmentación tecnológica dificulta la identificación de causas raíz, incrementa los tiempos de respuesta ante incidentes y limita la visibilidad en tiempo real de la salud de los servicios.

Adicionalmente, al no contar con una arquitectura de monitoreo diseñada formalmente, los flujos de información no están estandarizados y las dependencias entre sistemas críticos no están claramente definidas, lo cual representa un riesgo operativo y una barrera para la automatización. Esta situación impacta directamente en los procesos de análisis de eventos por parte del personal de Nivel 1 (N1) y Nivel 2 (N2), quienes requieren herramientas integradas y vistas consolidadas para ejecutar sus funciones con mayor eficiencia.

La inexistencia de una solución arquitectónica estandarizada no solo dificulta la gestión de incidentes y eventos, sino que también limita la capacidad de la organización para escalar sus operaciones, incorporar nuevas tecnologías o responder de manera ágil a cambios del entorno

tecnológico. Por lo tanto, se hace necesario abordar esta problemática mediante el diseño de una arquitectura técnica que sirva como base estructural para futuros desarrollos, integraciones y mejoras, sin entrar en su implementación práctica, respetando así el alcance académico y conceptual del proyecto SIMAI.

A lo anterior, se suma que la falta de integración efectiva entre las plataformas de monitoreo actualmente utilizadas (Zabbix, Dynatrace, Grafana, Kibana y Elasticsearch) genera una serie de desafíos adicionales:

- Duplicidad de esfuerzos y recursos: Los operadores deben consultar múltiples interfaces y sistemas para obtener una visión completa del estado de la infraestructura y las aplicaciones, lo que incrementa el riesgo de errores humanos y retrasa la toma de decisiones críticas.
- Dificultad en la correlación de eventos: La ausencia de una base de datos centralizada y de flujos de datos estandarizados impide correlacionar incidentes que afectan a diferentes capas tecnológicas (infraestructura, aplicaciones, seguridad), dificultando la identificación de causas raíz y la prevención de incidentes recurrentes.
- Limitaciones en la automatización y escalabilidad: Sin una arquitectura formal, resulta complejo implementar procesos automatizados de gestión de alertas, escalamiento de incidentes y generación de reportes, lo que limita la capacidad de la organización para adaptarse a un entorno de crecimiento y transformación digital.
- Riesgos de cumplimiento normativo y de seguridad: La dispersión de logs y eventos dificulta la trazabilidad, la auditoría y el cumplimiento de normativas como ISO/IEC 27001:2013, Ley 1581 de 2012 y la Circular 007 de 2018, exponiendo a la organización a sanciones y riesgos reputacionales.

- Impacto en la satisfacción del cliente y la competitividad: Los retrasos en la detección y resolución de incidentes afectan la calidad del servicio, la percepción del cliente y la posición competitiva de Global Hitss en el mercado de servicios gestionados de TI.

Justificación

Este proyecto se enmarca en las necesidades específicas del área de monitoreo de servicios de Global Hitss Colombia, donde la eficiencia operativa y la capacidad de respuesta ante incidentes son pilares fundamentales para mantener altos niveles de servicio a sus clientes. Global Hitss opera en un entorno altamente competitivo, lo que exige que sus operaciones de monitoreo sean ágiles, automatizadas y centralizadas, condiciones que actualmente no se cumplen en su totalidad debido a la dispersión de herramientas y a la falta de una arquitectura formal.

Además, la propuesta toma como base el marco de referencia ITIL (Information Technology Infrastructure Library), que no es una norma, sino una guía de buenas prácticas para la gestión eficiente de los servicios de TI. ITIL proporciona lineamientos esenciales para estructurar procesos como la gestión de incidentes, la gestión de problemas y la mejora continua del servicio. Al seguir este marco, el diseño arquitectónico no solo responde a necesidades técnicas, sino también organizacionales y estratégicas, alineándose con estándares globales de calidad en la prestación de servicios tecnológicos4.

En términos académicos, el desarrollo de este diseño arquitectónico sin entrar en su implementación práctica permite abordar un caso real enmarcado en una problemática concreta, aplicando herramientas de análisis y marcos conceptuales que refuerzan la formación profesional del estudiante. La orientación hacia Global Hitss Colombia asegura que el proyecto tenga pertinencia, aplicabilidad y relevancia tanto académica como profesional.

Desde el punto de vista normativo y de sostenibilidad, el diseño de SIMAI se alinea con los estándares internacionales de seguridad de la información, como ISO/IEC 27001:2013, y la legislación colombiana, como la Ley 1581 de 2012 y la Circular 007 de 2018 de la

Superintendencia Financiera. La arquitectura propuesta permite implementar controles de acceso, cifrado, auditoría y retención de logs conforme a las mejores prácticas y requerimientos legales, fortaleciendo la postura de seguridad y cumplimiento de la organización.

Por otra parte, la centralización y automatización del monitoreo contribuyen a reducir los tiempos de respuesta ante incidentes críticos, mejorar la correlación de eventos y fortalecer la toma de decisiones basada en datos. Esto no solo impacta positivamente en la satisfacción del cliente y en el cumplimiento de los acuerdos de nivel de servicio (SLA), sino que también incrementa la capacidad de la organización para adaptarse a cambios tecnológicos y regulatorios.

En términos de sostenibilidad tecnológica y responsabilidad ambiental, la utilización de servicios cloud como Azure permite optimizar el uso de recursos, reducir la huella de carbono y alinearse con prácticas de TI sustentable, como recomienda la literatura reciente. Además, la reutilización de herramientas ya existentes en la organización minimiza el impacto ambiental y los costos asociados a la adquisición de nuevas plataformas.

Finalmente, la importancia de este diseño radica en su capacidad para sentar las bases de una solución futura, escalable y alineada con las tendencias actuales en monitoreo inteligente, analítica de datos y automatización, contribuyendo de manera significativa al fortalecimiento de la infraestructura tecnológica de Global Hitss y a la consolidación de su posición como referente en la provisión de servicios gestionados de TI.

Análisis de Requerimientos

El diseño de la arquitectura del Sistema Integrado de Monitoreo y Análisis de Incidentes (SIMAI) requiere un análisis detallado de requerimientos que asegure el alineamiento con los objetivos propuestos, enfocados exclusivamente en la fase de diseño arquitectónico sin comprometer recursos al desarrollo. A continuación, se presenta este análisis estructurado:

Intención del Producto

SIMAI tiene como intención principal proporcionar una arquitectura de solución de monitoreo centralizada para Hitss Colombia que permita, una vez implementada, la detección, análisis y gestión de incidentes en tiempo real sobre la plataforma Microsoft Azure. La arquitectura propuesta integrará conceptualmente las herramientas existentes (Zabbix, Dynatrace, Grafana y Kibana) para superar las limitaciones actuales de falta de integración, gestión manual y dificultades en la correlación de eventos.

Se debe añadir que, además de las herramientas mencionadas, Elasticsearch también será considerada como fuente principal para el almacenamiento y búsqueda eficiente de grandes volúmenes de logs y eventos, integrando así las cinco plataformas clave del entorno de monitoreo actual de Global Hitss.

Herramientas y Servicios para el Diseño Arquitectónico

- Microsoft Azure Portal: Punto central para la conceptualización de todos los servicios de la solución.
- Azure Architecture Center: Para la utilización de patrones y prácticas recomendadas de diseño.
- Microsoft Visio/Lucidchart/Draw.io: Para la diagramación de la arquitectura propuesta.

- Azure Pricing Calculator: Para la estimación de costos del diseño propuesto.
- Zabbix, Dynatrace, Grafana, Kibana y Elasticsearch: Fuentes de datos y plataformas de monitoreo integradas en la arquitectura.

Requerimientos Funcionales para el Diseño Arquitectónico

Centralización de Monitoreo

Requerimiento: La arquitectura debe especificar cómo integrar datos provenientes de Zabbix, Dynatrace, Grafana, Kibana y Elasticsearch en una única plataforma.

Enfoque de Diseño: Modelado de flujos de datos e interfaces de integración entre las plataformas existentes.

Componentes Azure por Especificar:

- Azure Monitor: Como columna vertebral conceptual para la recopilación centralizada de métricas.
- Azure Log Analytics: Para el diseño del almacenamiento y consulta de logs.
- Azure Event Hub: Para el diseño de la ingesta en tiempo real de eventos.

Beneficios:

- Visibilidad unificada de la infraestructura, reduciendo la necesidad de cambiar entre diferentes interfaces.
- Correlación mejorada entre métricas de diferentes sistemas.
- Reducción del tiempo necesario para diagnosticar problemas complejos que afectan múltiples sistemas.

Ventajas:

- Preserva la inversión existente en herramientas especializadas.

- Permite aprovechar las fortalezas individuales de cada herramienta.
- Facilita la transición gradual hacia un sistema centralizado.

Desventajas:

- Complejidad en el diseño de interfaces de integración.
- Potenciales desafíos de sincronización entre sistemas.
- Puede requerir almacenamiento adicional para datos duplicados.

Origen y destino de datos en la arquitectura SIMAI

Herramienta	Tipo de dato	Protocolo/Integración	Destino en Azure
Zabbix	Métricas infra/NW	API, SNMP, agente	Event Hub, Log Analytics
Dynatrace	Trazas APM, alertas	API, OpenTelemetry	Log Analytics, Event Hub
Grafana	Dashboards, métricas	API, exportación JSON	Blob Storage, Data Explorer
Kibana	Logs estructurados	API, integración Elastic	Data Explorer, Log Analytics
Elasticsearch	Logs, eventos	API, integración nativa	Data Explorer, Log Analytics

Tabla 1. Descripción de orígenes de datos arquitectura SIMAI. Fuente: Diseño Propio

Gestión de Alertas e Incidentes (Diseño Conceptual)

Requerimiento: La arquitectura debe especificar cómo categorizar y priorizar automáticamente las alertas basándose en su criticidad.

Enfoque de Diseño: Modelado del flujo de procesamiento de alertas y definición de reglas de categorización.

Componentes Azure por especificar:

- Azure Alerts: Para el diseño de reglas de alerta basadas en condiciones predefinidas.
- Azure Logic Apps: Para el diseño del flujo de trabajo de notificaciones e integración.
- Azure Service Health: Para el diseño del monitoreo del estado de los servicios de Azure.

Beneficios:

- Reducción de "alert fatigue" mediante la priorización inteligente.
- Respuesta más rápida a incidentes críticos.
- Mejor asignación de recursos técnicos según la severidad del incidente.

Ventajas:

- Automatización del flujo de trabajo de alertas.
- Consistencia en la clasificación de incidentes.
- Alineación con mejores prácticas ITIL.

Desventajas:

- Requiere definición detallada de reglas de criticidad.
- Puede necesitar refinamientos continuos para evitar falsos positivos.
- Complejidad en la integración con sistemas de tickets existentes.

Análisis de Datos y Correlación (Diseño Conceptual)

Requerimiento: La arquitectura debe especificar cómo correlacionar eventos de diferentes fuentes para identificar patrones y causas raíz.

Enfoque de Diseño: Modelado de flujos de análisis y definición de patrones de correlación.

Componentes Azure Por Especificar:

- Azure Stream Analytics: Para el diseño del procesamiento en tiempo real.
- Azure Functions: Para el diseño de la lógica personalizada de análisis.
- Azure Data Explorer: Para el diseño del análisis de grandes volúmenes de datos.

Beneficios:

- Identificación más rápida de la causa raíz de incidentes complejos.
- Capacidad para detectar patrones emergentes antes de que causen incidentes.
- Insights que pueden informar decisiones de optimización de infraestructura.

Ventajas:

- Aprovecha capacidades avanzadas de análisis en la nube.
- Escalabilidad para manejar grandes volúmenes de datos.
- Flexibilidad para adaptar algoritmos de correlación.

Desventajas:

- Mayor complejidad en el diseño del flujo de datos.
- Potenciales costos elevados para procesamiento en tiempo real.
- Requiere expertise especializado para definir reglas de correlación efectivas.

Reportes y Dashboards (Diseño Conceptual)

Requerimiento: La arquitectura debe especificar cómo generar reportes personalizables sobre el estado de la infraestructura.

Enfoque de Diseño: Modelado de paneles de visualización y diseño conceptual de reportes.

Componentes Azure por especificar:

- Azure Workbooks: Para el diseño de informes interactivos.
- Azure Dashboards: Para la visualización rápida y centralizada.

Beneficios:

- Visibilidad mejorada para diferentes niveles organizacionales.
- Capacidad para personalizar vistas según roles específicos.
- Mejor comunicación de métricas clave a stakeholders.

Ventajas:

- Flexibilidad para crear múltiples tipos de visualizaciones.
- Capacidades de drill-down para análisis detallado.
- Opciones para exportación y distribución automática de reportes.

Desventajas:

- Complejidad en el diseño de dashboards efectivos.
- Potencial sobrecarga de información si no se diseña correctamente.

Gestión de Usuarios y Roles (Diseño Conceptual)

Requerimiento: La arquitectura debe especificar cómo implementar un control de acceso basado en roles.

Enfoque de Diseño: Modelado de la estructura de roles y permisos.

Componentes Azure por Especificar:

- Azure Active Directory: Para el diseño de la autenticación y gestión de identidades.
- Azure RBAC: Para la asignación de permisos específicos.
- Azure Activity Log: Para el registro de actividades y auditoría.

Beneficios:

- Seguridad mejorada mediante el principio de mínimo privilegio.
- Trazabilidad de acciones para auditoría y cumplimiento.
- Experiencia personalizada según el rol del usuario.

Ventajas:

- Integración con sistemas de identidad existentes.
- Flexibilidad para definir roles personalizados.
- Cumplimiento con normativas de seguridad.

Desventajas:

- Complejidad en la gestión de roles granulares.
- Potencial impacto en la usabilidad si es demasiado restrictivo.
- Requiere mantenimiento continuo a medida que cambian las responsabilidades.

Requerimientos No Funcionales para el Diseño Arquitectónico

Historias de Usuario

A continuación, se presenta una tabla detallada de historias de usuario, alineadas con los objetivos y requerimientos del proyecto, considerando las cinco herramientas principales:

ID	Rol	Necesidad	Herramienta origen	Beneficio	Criterios de aceptación principales
HU1	Operador N1	Visualizar alertas centralizadas de Zabbix, Dynatrace, Grafana, Kibana y Elasticsearch	Zabbix, Dynatrace, Grafana, Kibana, Elasticsearch	Reducir tiempos de respuesta	Panel en tiempo real, filtrado por origen, autenticación Azure AD
HU2	Líder de monitoreo	Generar reportes y dashboards automáticos	Grafana, Kibana, Azure	Cumplir SLA y tomar decisiones informadas	Dashboards históricos, programación de reportes, exportación PDF/Excel
HU3	Administrador de TI	Gestionar permisos y roles con Azure AD	Azure AD, RBAC	Seguridad y cumplimiento normativo	Roles predefinidos, logs de auditoría, MFA
HU4	Analista de incidentes	Correlacionar eventos de diferentes fuentes en tiempo real	Todas	Identificar causa raíz y prevenir recurrencia	Línea de tiempo, alertas inteligentes, latencia máxima de 2 minutos
HU5	Responsable de seguridad	Auditar todas las acciones de los usuarios	Azure Activity Log	Garantizar trazabilidad y cumplimiento legal	Log inalterable, alertas de acceso no autorizado, retención de cinco años

Tabla 2: Historias de Usuario. Fuente: Diseño propio

Matriz de Trazabilidad de Requerimientos

ID Req.	Descripción del Requerimiento	Historia de Usuario Relacionada	Objetivo Específico Relacionado	Herramienta/Componente Azure
RF-01	Integración centralizada de alertas y métricas	HU1, HU4	Definir requerimientos funcionales	Event Hub, Log Analytics, Azure Monitor
RF-02	Automatización de reportes y dashboards	HU2	Generar reportes y dashboards	Azure Workbooks, Azure Dashboards
RF-03	Control de acceso basado en roles (RBAC)	HU3, HU5	Seguridad y trazabilidad	Azure AD, RBAC, Activity Log
RF-04	Correlación de eventos multifuente	HU4	Correlación y análisis de eventos	Stream Analytics, Data Explorer
RNF-01	Disponibilidad mínima del 99.9%	Todos los usuarios	Escalabilidad y disponibilidad	Arquitectura redundante
RNF-02	Cumplimiento de ISO/IEC 27001:2013	HU5	Seguridad y cumplimiento normativo	Logs de auditoría, cifrado

Tabla 3. Trazabilidad de Requerimientos. Fuente: Diseño propio.

Marco Teórico

Global Hitss es una empresa multinacional de servicios de tecnología, filial del grupo América Móvil, con presencia en más de 15 países de América Latina. En Colombia, Global Hitss se ha consolidado como un actor estratégico en la provisión de soluciones tecnológicas, servicios de outsourcing, consultoría y soporte TI para sectores como telecomunicaciones, banca, gobierno y servicios públicos. La compañía está enfocada en proveer servicios gestionados que aseguren la disponibilidad, rendimiento y continuidad de los sistemas informáticos y plataformas digitales de sus clientes.

Dentro de sus principales líneas de operación se encuentran la atención y soporte a usuarios (N1 y N2), monitoreo de infraestructura, gestión de redes, mantenimiento de aplicaciones, automatización de procesos y desarrollo de software bajo demanda. El área de monitoreo, foco de este proyecto, opera con múltiples herramientas como Zabbix, Dynatrace, Grafana y Kibana, que permiten supervisar eventos, métricas de rendimiento, logs, y flujos de red. Sin embargo, esta diversidad de plataformas genera dispersión en la gestión de información, duplicidad de esfuerzos y limitaciones para lograr una visión unificada del estado de los servicios.

A nivel técnico, la arquitectura de monitoreo moderna requiere la integración de múltiples fuentes de datos y la centralización de la visualización y el análisis. En el caso de SIMAI, se consideran cinco herramientas fundamentales:

- Zabbix: utilizada para el monitoreo de infraestructura, servidores y dispositivos de red, con capacidad de generar alertas y reportes en tiempo real.

- Dynatrace: orientada al monitoreo de aplicaciones, análisis de rendimiento y trazabilidad de transacciones mediante inteligencia artificial.
- Grafana: plataforma de visualización de métricas y generación de dashboards personalizables, que facilita la interpretación de datos operativos.
- Kibana: herramienta gráfica del stack ELK, especializada en la visualización avanzada de logs estructurados y análisis forense de eventos.
- Elasticsearch: motor de búsqueda y almacenamiento de grandes volúmenes de datos, que permite indexar, consultar y correlacionar eventos de diversas fuentes.

La integración de estas herramientas con servicios nativos de Azure (Monitor, Log Analytics, Event Hub, Data Explorer) es clave para lograr la centralización, automatización y escalabilidad del monitoreo, alineando la solución con los estándares internacionales de seguridad (ISO/IEC 27001:2013) y las mejores prácticas de ITIL v4 para la gestión de servicios TI.

El concepto de arquitectura de monitoreo se refiere al conjunto estructurado de componentes, relaciones, interfaces y procesos que permiten observar, medir, analizar y actuar sobre la operación de sistemas tecnológicos en tiempo real (Bass, Clements & Kazman, 2012). A diferencia de una simple herramienta de supervisión, una arquitectura de monitoreo integra múltiples fuentes de información, establece reglas de correlación, automatiza respuestas y proporciona dashboards inteligentes orientados a la toma de decisiones.

En el caso de Global Hitss Colombia, una arquitectura bien diseñada debe permitir la interoperabilidad entre herramientas como Dynatrace (observabilidad basada en inteligencia artificial), Zabbix (monitoreo de infraestructura), Grafana (visualización de métricas), Kibana (análisis de logs) y Elasticsearch (almacenamiento y búsqueda avanzada). Además, debe

contemplar aspectos como alta disponibilidad, tolerancia a fallos, escalabilidad horizontal, y cumplimiento de normas de seguridad de la información (como ISO/IEC 27001).

La arquitectura debe facilitar la integración nativa con Azure, permitiendo la ingesta de datos y eventos de Zabbix, Dynatrace y Elasticsearch en Azure Monitor y Log Analytics, así como la visualización avanzada en Grafana y Kibana. Según la documentación oficial de Elastic, Kibana y Elasticsearch pueden integrarse con Azure para observabilidad y análisis a escala, permitiendo correlación de logs, métricas y trazas en entornos híbridos y cloud.

Benchmarking y soluciones similares:

En el mercado existen soluciones comerciales robustas como Splunk Enterprise, IBM Netcool Operations Insight, ServiceNow ITOM y la propia plataforma de Dynatrace, que ofrecen capacidades avanzadas de monitoreo, correlación y análisis predictivo. Sin embargo, estas soluciones suelen tener altos costos de licenciamiento, complejidad de implementación y dependencia de proveedores externos. El enfoque de SIMAI es aprovechar las herramientas ya presentes en Global Hitss, integrándolas mediante servicios nativos de Azure para lograr una solución personalizada, escalable y alineada con las necesidades reales de la organización.

El marco de referencia ITIL (Information Technology Infrastructure Library) representa uno de los pilares fundamentales para estructurar servicios de TI bajo principios de calidad, eficiencia y mejora continua. ITIL.

El concepto de observabilidad ha evolucionado en el contexto de la ingeniería de software moderna como una extensión del monitoreo tradicional, al incluir análisis de trazas, eventos, logs y métricas en tiempo real para obtener una visión holística del comportamiento del sistema. En lugar de esperar que una métrica dispare una alerta, los sistemas observables

permiten comprender causas raíz, identificar patrones de fallo y generar conocimiento accionable.

Uno de los principios esenciales del diseño arquitectónico en entornos empresariales como Global Hitss es la sostenibilidad tecnológica. Esta se refiere a la capacidad del sistema para adaptarse a nuevas tecnologías, aumentar su capacidad operativa y mantenerse funcional ante cambios del entorno sin requerir rediseños completos. En ese sentido, el diseño de SIMAI debe considerar la modularidad de sus componentes, la capacidad de integración con APIs, y el uso de estándares abiertos para asegurar su evolución a futuro.

Análisis de restricciones

Los problemas de ingeniería pueden tener muchísimas soluciones. Los ingenieros resuelven diversos problemas que tiene la sociedad, la industria, se habla de 104 soluciones para un problema específico. Al realizar el análisis de restricciones se debe revisar información de carácter técnico, normativo, económico, social, ambiental y cartográfico. De todas las soluciones que se puedan tener, la ingeniería encuentra restricciones como las siguientes:

Restricciones Ambientales

El desarrollo de SIMAI implica principalmente una solución digital basada en la nube de Azure, lo que reduce significativamente el impacto ambiental directo. Sin embargo, existen consideraciones ambientales importantes:

- **Consumo energético de centros de datos:** La arquitectura propuesta utiliza servicios cloud que operan en centros de datos con alto consumo energético. Microsoft se ha comprometido a utilizar energía 100% renovable para sus centros de datos para 2025, lo que alinea el proyecto con políticas de sostenibilidad.
- **Huella de carbono digital:** El procesamiento de grandes volúmenes de datos genera una huella de carbono. Cada GB de datos en la nube puede generar hasta 0.06 kg de CO_2. Considerando que SIMAI procesará aproximadamente 10,000 eventos por minuto, la huella ambiental debe ser monitoreada.
- **Cumplimiento normativo ambiental en Colombia:** El proyecto debe adherirse a la Resolución 0256 de 2018 del Ministerio de Ambiente y Desarrollo Sostenible de

Colombia, que establece los indicadores de seguimiento al uso de recursos naturales en proyectos tecnológicos.

- **Utilización de recursos existentes:** La solución propuesta integrará herramientas ya implementadas (Zabbix, Dynatrace, Grafana, Kibana y Elasticsearch), favoreciendo la reutilización sobre el desarrollo de nuevos sistemas, lo que representa una ventaja desde la perspectiva ambiental.

Restricciones Ambientales

Restricción	Descripción	Impacto en SIMAI	Mitigación/Control
Consumo energético de centros de datos	Uso intensivo de electricidad para operación y refrigeración de servidores cloud	Aumenta huella de carbono	Uso de Azure con energía renovable y monitoreo de consumo
Huella de carbono digital	Emisión de CO_2 por procesamiento y almacenamiento de datos en la nube	Contribuye al cambio climático	Optimización de recursos y políticas de eficiencia
Cumplimiento normativo ambiental	Adherencia a regulaciones colombianas sobre uso de recursos y sostenibilidad	Obligatorio para proyectos tecnológicos	Seguimiento a la Resolución 0256 de 2018
Reutilización de recursos existentes	Integración de herramientas ya implementadas (Zabbix, Dynatrace, Grafana, Kibana, Elasticsearch)	Reduce impacto ambiental y costos	Priorización de integración sobre adquisición nueva

Tabla 4: Descripción de restricciones ambientales. Fuente: Diseño propio

Restricciones Económicas

El desarrollo de SIMAI como solución interna frente a la adquisición de soluciones comerciales presenta varias consideraciones económicas:

- **Presupuesto disponible vs. necesidad de inversión:** Soluciones comerciales como Splunk Enterprise o IBM Netcool tienen costos anuales elevados. El desarrollo interno de SIMAI requiere una inversión inicial estimada en USD 80,000, con un costo operativo anual aproximado de USD 35,000 en servicios Azure.
- **Contexto macroeconómico colombiano:** Inflación (7.4% en marzo de 2025) y volatilidad del peso colombiano frente al dólar (tasa promedio de 4,200 COP/USD) afectan los costos fijos en moneda extranjera.
- **Beneficios financieros proyectados:** La implementación de SIMAI podría reducir hasta en un 42% los costos operativos asociados al manejo manual de incidentes, generando un ahorro anual estimado de USD 120,000 por mejora en la eficiencia y disponibilidad de servicios.
- **Riesgos financieros:** La fluctuación de precios en los servicios Azure (incrementos anuales del 5-10%) representa un riesgo para el presupuesto operativo a largo plazo.

Restricciones Económicas

Restricción	Descripción	Impacto en SIMAI	Estrategia de Mitigación
Presupuesto limitado	Recursos económicos asignados al proyecto	Puede limitar alcance o calidad	Priorización de fases y optimización de recursos
Volatilidad cambiaria	Fluctuación del COP/USD afecta costos de servicios cloud	Incremento de costos operativos	Contratos a largo plazo y reservas presupuestales
Costos de licenciamiento	Herramientas comerciales pueden tener costos elevados	Aumenta el TCO	Uso de herramientas open source y licencias existentes

Riesgos de sobrecostos	Cambios en tarifas de Azure y servicios asociados	Riesgo de exceder presupuesto	Monitoreo y control de costos en tiempo real

Tabla 5: Descripción de restricciones económicas. Fuente: Diseño propio.

Restricciones Legales

El proyecto SIMAI debe considerar el marco legal colombiano y cumplir con diversas regulaciones:

- **Ley 1581 de 2012 (Protección de Datos Personales):** La centralización de información de múltiples sistemas podría implicar el manejo de datos personales, requiriendo medidas específicas de seguridad y consentimiento.
- **Circular 007 de 2018 de la Superintendencia Financiera:** El sistema debe cumplir con los requisitos de ciberseguridad establecidos para la infraestructura crítica del sector financiero.
- **Decreto 1008 de 2018 (Política de Gobierno Digital):** Aplica a entidades que prestan servicios al sector público.
- **Acuerdos contractuales con clientes:** Los SLA existentes pueden limitar ciertas implementaciones o requerir procesos de aprobación adicionales.
- **Regulaciones internacionales:** El almacenamiento de datos en centros ubicados en EE.UU. y Brasil debe cumplir con normativas como el GDPR y la LGPD.

Restricciones Legales

Restricción	Descripción	Impacto en SIMAI	Mitigación/Control
Protección de datos personales	Ley 1581 de 2012 exige medidas de seguridad y consentimiento	Obligatorio para manejo de datos	Enmascaramiento, cifrado y políticas de privacidad
Ciberseguridad en sector financiero	Circular 007/2018 exige controles específicos	Requiere auditoría y monitoreo continuo	Implementación de controles ISO/IEC 27001:2013
Cumplimiento de gobierno digital	Decreto 1008/2018 establece lineamientos para servicios públicos	Aplicable a clientes del sector público	Alineación con políticas de gobierno digital
Regulaciones internacionales	GDPR y LGPD para clientes internacionales	Restricciones en almacenamiento y transferencia	Implementación de políticas de compliance y localización de datos

Tabla 6: Descripción de restricciones Legales. Fuente: Diseño propio.

Restricciones de Salud y Seguridad

Aunque SIMAI es principalmente un sistema digital, existen consideraciones de salud y seguridad:

- **Seguridad de la información:** El sistema manejará información crítica sobre la infraestructura tecnológica de Hitss Colombia y sus clientes, lo que implica riesgos de seguridad que deben mitigarse mediante controles adecuados según ISO/IEC 27001:2013.
- **Ergonomía y salud ocupacional:** El diseño de las interfaces debe considerar principios ergonómicos para prevenir problemas de salud en los operadores.
- **Continuidad operativa:** SIMAI monitorea sistemas críticos cuya interrupción podría tener implicaciones para la salud y seguridad en ciertos sectores.

- **Protección contra incidentes de ciberseguridad:** Se deben implementar mecanismos robustos para prevenir que vulnerabilidades en el sistema de monitoreo se conviertan en vectores de ataque.

Restricciones de Salud y Seguridad

Restricción	Descripción	Impacto en SIMAI	Estrategia de Mitigación
Seguridad de la información	Manejo de datos críticos y confidenciales	Riesgo de brechas de seguridad	Controles de acceso, cifrado, auditoría
Ergonomía y salud ocupacional	Uso prolongado de interfaces por operadores de monitoreo	Riesgo de fatiga y lesiones	Diseño ergonómico y pausas programadas
Continuidad operativa	Interrupción de servicios críticos	Riesgo para sectores sensibles	Alta disponibilidad y planes de contingencia
Incidentes de ciberseguridad	Vulnerabilidades explotables en el sistema	Riesgo de ataques y sabotaje	Actualizaciones, pruebas de penetración

Tabla 7: Descripción de restricciones de salud y seguridad. Fuente: Diseño propio.

Restricciones Socioculturales

La implementación de SIMAI implica cambios en los hábitos de trabajo que deben considerarse:

- **Resistencia al cambio:** Los equipos técnicos han desarrollado rutinas basadas en herramientas actuales. La transición a un sistema centralizado puede generar resistencia, requiriendo un plan de gestión del cambio.
- **Cultura organizacional:** La empresa tiene una cultura técnica orientada a soluciones específicas (Zabbix para infraestructura, Dynatrace para aplicaciones, etc.). La adopción de una plataforma unificada requerirá adaptación cultural y formación.
- **Cambios en roles y responsabilidades:** La automatización modificará las responsabilidades de los equipos de monitoreo N1 y N2.

- **Expectativas de los clientes:** Cambios en la presentación de información deben gestionarse para mantener la satisfacción.

Restricciones Socioculturales

Restricción	Descripción	Impacto en SIMAI	Estrategia de Mitigación
Resistencia al cambio	Cambios en rutinas y herramientas	Dificultad en adopción	Plan de gestión del cambio, capacitación
Cultura organizacional	Orientación a herramientas específicas	Adaptación cultural necesaria	Comunicación y formación continua
Cambios en roles	Automatización de tareas operativas	Redefinición de funciones	Rediseño de procesos y capacitación
Expectativas de clientes	Cambios en informes y alertas entregados	Riesgo de insatisfacción	Gestión de expectativas y retroalimentación

Tabla 8: Descripción de restricciones socioculturales. Fuente: Diseño propio.

Restricciones Técnicas Adicionales

- **Integración con sistemas legacy:** Diferentes protocolos y formatos de datos requieren adaptadores específicos.
- **Limitaciones de API:** Algunas herramientas tienen APIs limitadas, restringiendo la integración en tiempo real.
- **Latencia entre regiones**: La distribución geográfica puede generar desafíos de latencia para la consolidación de datos.
- **Escalabilidad heterogénea:** Patrones de crecimiento distintos entre componentes complican la planificación de capacidad.

- **Disponibilidad de talento:** Escasez de especialistas en Azure y sistemas de monitoreo integrados en Colombia.

Restricciones Técnicas

Restricción	Descripción	Impacto en SIMAI	Estrategia de Mitigación
Integración con sistemas legacy	Diferentes protocolos y formatos de datos	Dificultad de integración	Uso de adaptadores y middleware
Limitaciones de API	APIs restringidas en algunas herramientas	Limitación en integración en tiempo real	Desarrollo de soluciones alternativas
Latencia entre regiones	Distribución geográfica de servicios Azure	Posible retraso en consolidación	Optimización de red y replicación
Escalabilidad heterogénea	Diferente crecimiento de componentes	Complejidad en planificación	Monitoreo y ajuste dinámico de recursos
Disponibilidad de talento	Escasez de especialistas en tecnologías requeridas	Riesgo en desarrollo y mantenimiento	Capacitación y contratación especializada

Tabla 9: Descripción de restricciones técnicas. Fuente: Diseño propio.

Metodología para la selección y desarrollo de la solución

El diseño arquitectónico del proyecto SIMAI, enfocado en el entorno real de monitoreo de Global Hitss Colombia, requiere una metodología robusta que no solo permita estructurar técnicamente la solución, sino también garantizar su alineación con los objetivos estratégicos de la organización y las buenas prácticas globales. Teniendo en cuenta que el proyecto se limita al diseño conceptual sin llegar al desarrollo de la solución, la metodología debe enfocarse en marcos de referencia que guíen una arquitectura sólida, escalable, resiliente y adaptable a ambientes de nube como Microsoft Azure, que es la plataforma prevista para la futura implementación.

Criterios de selección metodológica

La selección de los marcos metodológicos para este proyecto se basa en los siguientes criterios:

- Compatibilidad con entornos de nube (Azure).
- Enfoque en diseño arquitectónico, no en desarrollo o implementación.
- Adaptabilidad a entornos empresariales de alta disponibilidad y operación continua.
- Alineación con las mejores prácticas internacionales en arquitectura de TI y monitoreo.
- Relevancia para procesos de observabilidad, trazabilidad, escalabilidad y automatización.

Además, la metodología seleccionada debe permitir la integración de herramientas heterogéneas (Zabbix, Dynatrace, Grafana, Kibana, Elasticsearch) y garantizar que la arquitectura propuesta sea auditable, segura y alineada con los marcos regulatorios y normativos aplicables en Colombia y a nivel internacional.

Azure Well-Architected Framework

El Azure Well-Architected Framework es un conjunto de principios y buenas prácticas desarrolladas por Microsoft para ayudar a los arquitectos de soluciones en la nube a diseñar, construir y mantener sistemas confiables, seguros y eficientes en Azure. Este marco se articula en cinco pilares fundamentales: confiabilidad, seguridad, eficiencia operativa, rendimiento y optimización de costos (Microsoft, 2023).

En el caso de Global Hitss, estos pilares son fundamentales para el entorno de monitoreo, que debe operar con altos niveles de disponibilidad y confiabilidad. Por ejemplo, la confiabilidad es esencial para asegurar la continuidad del monitoreo 24/7; la eficiencia operativa garantiza la automatización y reducción de errores humanos; y la optimización de costos permite escalar sin generar sobrecargas presupuestales.

El marco de Microsoft permite evaluar arquitecturas mediante evaluaciones específicas (Well-Architected Review), lo cual es valioso en un proyecto como SIMAI, donde se busca proponer una solución sólida para evaluación futura, aunque no se implementará en esta fase. Esto facilita una aproximación rigurosa al diseño, integrando herramientas nativas de Azure que Global Hitss podría aprovechar a mediano plazo.

The Twelve-Factor App

Aunque originalmente concebido para el desarrollo de aplicaciones como servicio (SaaS), el modelo The Twelve-Factor App proporciona principios arquitectónicos clave que pueden aplicarse en el diseño de sistemas distribuidos y monitorizados. Entre sus factores más relevantes para SIMAI destacan:

- Configuración por entorno: Separa la configuración del código, lo cual es esencial para entornos multicliente como los que gestiona Global Hitss.

- Procesos aislados: Permite el diseño modular de la solución de monitoreo, facilitando el mantenimiento y la escalabilidad.
- Logs como flujos de eventos: Este principio se alinea con los sistemas de observabilidad y registros utilizados actualmente (como Grafana, Kibana y Dynatrace), permitiendo una centralización coherente del registro de eventos.

Este marco metodológico es especialmente útil en SIMAI porque promueve la portabilidad, la replicabilidad y la resiliencia. Aunque no se desarrollará una aplicación, sí se diseña una arquitectura que puede, en el futuro, acoger componentes que se beneficien de esta estructura lógica. Además, proporciona criterios de diseño sostenibles para entornos dinámicos como Azure.

TOGAF + Cloud Adaptations

TOGAF (The Open Group Architecture Framework) es uno de los marcos de arquitectura empresarial más ampliamente utilizados en el mundo. Su enfoque basado en fases (ADM – Architecture Development Method) permite estructurar de forma metódica los componentes de una arquitectura desde las fases preliminares hasta la planificación de la migración y el gobierno del sistema (The Open Group, 2022).

Para el caso de Global Hitss, la adaptación de TOGAF al entorno de nube resulta particularmente relevante. Esta organización opera en sectores sensibles como banca y telecomunicaciones, por lo que requiere una arquitectura robusta, escalable y con altos niveles de trazabilidad y seguridad. TOGAF, combinado con las adaptaciones a entornos de nube propuestas por publicaciones recientes, permite:

- Definir claramente los dominios de arquitectura (negocio, datos, aplicaciones y tecnología).

- Establecer puntos de control y gobernanza que aseguren la calidad y escalabilidad de la solución.
- Facilitar la interoperabilidad entre plataformas actuales (Zabbix, Dynatrace, Grafana, Kibana, Elasticsearch) bajo una estructura unificada.

Este marco permite también vincular el diseño con las estrategias empresariales de mejora continua, automatización y eficiencia operativa, pilares estratégicos identificados en la definición del problema.

Proceso metodológico aplicado

Fase	Actividades principales	Herramientas y marcos aplicados
Levantamiento de requerimientos	Entrevistas, análisis de procesos actuales, revisión de documentación, identificación de flujos de monitoreo y eventos.	TOGAF (fase preliminar), ITIL
Diseño conceptual	Modelado de componentes, definición de flujos de datos, selección de servicios Azure, integración de herramientas de monitoreo.	Azure Well-Architected, Twelve-Factor App
Evaluación de alternativas	Comparativa de soluciones comerciales y open source, análisis de ventajas y desventajas, estimación de costos y riesgos.	TOGAF (ADM), benchmarking
Validación del diseño	Revisión con stakeholders, simulación de escenarios, análisis de cumplimiento normativo y técnico.	Azure Well-Architected Review, ITIL
Documentación y mejora	Elaboración de diagramas, matrices de trazabilidad, DOFA, PESTLE y recomendaciones para implementación futura.	TOGAF, mejores prácticas de documentación

Tabla 10: Metodología. Fuente: Diseño propio.

Comparativa de marcos metodológicos

Marco metodológico	Propósito principal	Aplicación en SIMAI	Beneficio clave
Azure Well-Architected	Buenas prácticas para arquitectura cloud en Azure	Evaluación de confiabilidad, seguridad, costos, rendimiento	Solidez técnica y alineación cloud
Twelve-Factor App	Principios para sistemas distribuidos y escalables	Modularidad, gestión de logs, escalabilidad y portabilidad	Flexibilidad y resiliencia
TOGAF + Cloud Adaptations	Estructuración de arquitectura empresarial	Definición de dominios, fases y gobernanza	Alineación estratégica y gobernanza

Tabla 11: Marcos Metodológicos - Comparación. Fuente: Diseño propio.

Instrumentos de recolección de información

- Entrevistas estructuradas con usuarios N1, N2 y líderes de monitoreo.
- Revisión documental de procesos actuales y SLAs.
- Cuestionarios técnicos para identificar necesidades de integración y seguridad.
- Análisis de benchmarking con soluciones comerciales y open source.
- Workshops de validación con stakeholders para retroalimentación iterativa.

La integración de estos tres marcos metodológicos permite una aproximación holística y precisa al problema que enfrenta Global Hitss. Cada marco aporta ventajas específicas que, combinadas, resultan en un diseño arquitectónico coherente, sustentado, escalable y adaptable a la nube, cumpliendo con los objetivos estratégicos y los estándares internacionales de arquitectura de TI y monitoreo.

Análisis de costos

En la planeación de un proyecto tecnológico como SIMAI, que busca diseñar e implementar una arquitectura de monitoreo en la nube (Azure) con soporte de estándares ITIL y tecnologías como Elastic, Grafana, Dynatrace y Zabbix, es crucial realizar un análisis de costos preciso. Este análisis no solo permite anticipar la inversión necesaria, sino que también facilita la toma de decisiones estratégicas para asegurar la viabilidad económica del proyecto.

Clasificación General de Costos en el Proyecto SIMAI

Tal como se indica en la teoría de costos para ingeniería, se deben considerar tres categorías clave:

- **Costos directos**
- **Costos indirectos**
- **Capital de trabajo**

A continuación, se detallan estas categorías en el contexto del proyecto SIMAI.

Costos Directos

Recursos de infraestructura en Azure

Como el proyecto SIMAI no contempla el desarrollo de software sino el diseño de una arquitectura para implementación en Azure, uno de los principales costos directos está vinculado con los recursos en la nube. Esto incluye:

- Instancias de máquina virtual (VMs) para ambientes de pruebas y producción.
- Servicios de almacenamiento (Blob Storage y Azure Files) para logs de monitoreo.
- Uso de Azure Monitor, Log Analytics y Application Insights, necesarios para la integración de herramientas como Dynatrace y Zabbix.

Estimado mensual (ejemplo real):

Recurso Azure	Cantidad	Costo unitario (USD/mes)	Subtotal (USD/mes)
VM Standard D2s v3	2	$ 80	$ 160
Azure Blob Storage (1TB)	1	$ 23	$ 23
Azure Log Analytics (100GB)	1	$ 25	$ 25
Azure Event Hub (1 unidad básica)	1	$ 11	$ 11
Azure Aplicación Insight	1	$ 20	$ 20
Total, mensual estimado			**$ 239**

Tabla 12: Estimación de Costos - Mes a Mes. Fuente: Diseño propio.

Licencias y herramientas externas

Aunque muchas herramientas como Zabbix y Grafana son de código abierto, se contemplan licencias empresariales o versiones premium en el caso de:

- **Dynatrace:** se estima un costo de entre $21 y $69 USD por host monitoreado, dependiendo del alcance.
- **Elastic Observability:** si se requiere versión gestionada (Elastic Cloud), tiene un costo de aproximadamente $95 USD/mes por nodo.

Licenciamiento y herramientas externas:

Herramienta	Licencia/Versión	Costo mensual (USD)	Costo anual (USD)
Dynatrace	SaaS (10 hosts)	$ 690	$ 8.280,00
Elastic Cloud	2 nodos	$ 190	$ 2.280,00
Zabbix	Open Source	$ 0	$ 0
Grafana	Open Source	$ 0	$ 0
Kibana	Incluida en Elastic	$ 0	$ 0
Total, anual			**$ 10.560,00**

Tabla 13: Costo de licenciamiento. Fuente: Diseño propio.

Costos Indirectos

Los costos indirectos no se relacionan directamente con la infraestructura, pero son esenciales para el desarrollo del proyecto:

- **Permisos y cumplimiento de normativas:** Consultoría para alineación de arquitectura a marcos de referencia (TOGAF, Azure Well-Architected Framework). Formación del personal en buenas prácticas de ITIL y seguridad.
- **Costos estimados:**
    - Consultoría externa (40 horas): $2,000 USD.
    - Capacitación y certificación ITIL v4 Foundation (3 empleados): $1,200 USD.
- **Gastos generales (overhead):** Costos administrativos, como gerencia de proyecto, reuniones de seguimiento, supervisión técnica y gestión documental. Publicidad interna o difusión del proyecto dentro de Global Hitss.
    - Cálculo estimado overhead mensual: $1,500 USD.

Capital de Trabajo

Recursos humanos

- Diseño de arquitectura cloud.
- Pruebas funcionales del sistema.
- Documentación técnica.

Estimación para 3 meses:

Rol	Cantidad	Salario mensual (USD)	Subtotal (USD/3 meses)
Arquitecto de soluciones	1	$ 3.000,00	$ 9.000,00
Ingeniero de monitoreo	2	$ 2.000,00	$ 12.000,00
Analista de datos	1	$ 2.200,00	$ 6.600,00
Documentador técnico	1	$ 1.500,00	$ 4.500,00
Total, capital de trabajo			**$ 32.100,00**

Tabla 14: Estimación salarios -Mes. (tres meses). Fuente: Diseño Propio.

Insumos operativos

- Licencias temporales de software para pruebas.
- Espacios de coworking o alquiler de salas (si es presencial).
- Costos de conexión o equipos temporales para pruebas.

Estimación Global del Costo del Proyecto SIMAI (3 meses)

Categoría	Subtotal (USD)
Costos directos	$ 10.560,00
Costos indirectos	$ 6.200,00
Capital de trabajo	$ 32.100,00
Total, estimado	**$ 48.860,00**

Tabla 15: Estimación Global. Fuente: Diseño propio.

Comparativa con Soluciones Comerciales

Solución Comercial	Costo anual (USD)	Ventaja SIMAI
Splunk Enterprise	$45.000 - $150.000	Ahorro del 60% con arquitectura propia
IBM Netcool Operations	$70.000 - $200.000	Personalización y menor dependencia
ServiceNow ITOM	$60.000 - $120.000	Integración nativa con herramientas existentes
Dynatrace SaaS (20 hosts)	$ 46.560	Integración con Azure y Elastic

Tabla 16: Descripción de soluciones comerciales. Fuente: Diseño propio

Consideraciones adicionales

- Optimización de costos: El uso de herramientas open source y licencias ya existentes reduce el TCO (Total Cost of Ownership).

- Escalabilidad: Los costos pueden aumentar si la infraestructura o el volumen de datos crecen, por lo que se recomienda monitorear el uso y ajustar servicios bajo demanda.
- Sostenibilidad: La reutilización de recursos y la integración gradual permiten distribuir inversiones en el tiempo.

Diseño de la Arquitectura de Software

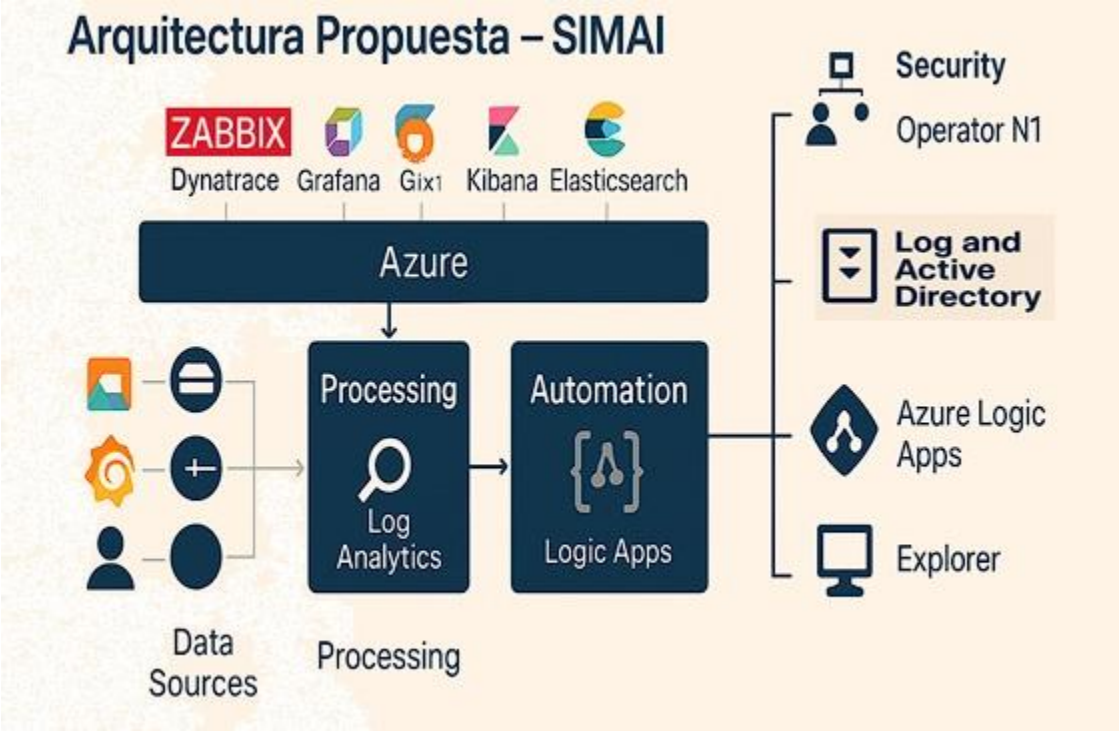

Ilustración 1: Propuesta de diseño de arquitectura. Fuente: Diseño propio.

Descripción General

La arquitectura de software del Sistema Integrado de Monitoreo y Análisis de Incidentes (SIMAI) para Global Hitss Colombia está diseñada para centralizar y automatizar el monitoreo, la correlación y la gestión de incidentes provenientes de cinco fuentes principales: Zabbix, Dynatrace, Grafana, Kibana y Elasticsearch. Todo el procesamiento, almacenamiento, automatización y visualización se realiza en la nube de Microsoft Azure, garantizando escalabilidad, seguridad, cumplimiento normativo y eficiencia operativa.

Explicación del Diagrama de Arquitectura

La arquitectura, basada en el diagrama adjunto, se compone de las siguientes capas y componentes:

Fuentes de Datos y Monitoreo

- **Zabbix, Dynatrace, Grafana, Kibana, Elasticsearch:**

  Son los sistemas de monitoreo y observabilidad actualmente implementados en Global Hitss. Cada uno recolecta métricas, logs, trazas y eventos de diferentes dominios (infraestructura, aplicaciones, seguridad, etc.).

- **Flujo de datos:**

  Cada herramienta envía sus datos hacia la nube de Azure mediante conectores, APIs o agentes, asegurando la captura en tiempo real o en lotes según la criticidad.

Plataforma Centralizada en Azure

- **Azure (Capa de integración principal):**

  Aquí convergen todos los datos provenientes de las herramientas de monitoreo. Azure actúa como el núcleo de integración, permitiendo la gestión centralizada y la interoperabilidad entre sistemas heterogéneos.

Procesamiento y Almacenamiento

- **Processing (Azure):**

  Primera etapa de procesamiento, donde los datos brutos de Zabbix, Dynatrace, Grafana, Kibana y Elasticsearch son normalizados y preparados para su análisis.

- **Processing (Log Analytics):**

  Los datos procesados se almacenan y analizan en Azure Log Analytics, que permite

consultas avanzadas, correlación de eventos, análisis histórico y generación de insights operativos.

- **Automation (Logic Apps):**

  Azure Logic Apps automatiza flujos de trabajo críticos, como la generación de alertas, la apertura de tickets en sistemas externos (ej. ServiceNow), y la orquestación de respuestas automáticas ante incidentes detectados.

Seguridad y Acceso

- **Operator N1:**

  Usuario principal encargado de la operación diaria del monitoreo.

- **Azure Active Directory:**

  Proporciona autenticación, autorización y control de acceso basado en roles (RBAC) para todos los usuarios y servicios, garantizando cumplimiento con ISO/IEC 27001 y la Ley 1581 de 2012.

- **Azure Logic Apps:**

  Además de la automatización, se integra con sistemas de gestión de identidades y flujos de aprobación.

Visualización y Exploración

- **Explorer:**

  Representa los dashboards y paneles interactivos construidos con Azure Workbooks, Azure Dashboards y/o Azure Managed Grafana, donde los operadores, líderes y responsables de seguridad pueden consultar en tiempo real el estado de la infraestructura, aplicaciones y eventos críticos.

Flujo de Datos y Procesos

1. **Recolección y envío:**

   Las herramientas Zabbix, Dynatrace, Grafana, Kibana y Elasticsearch recolectan eventos, métricas y logs desde los sistemas de Global Hitss y los envían a Azure mediante conectores seguros.

2. **Procesamiento inicial:**

   Azure recibe los datos, los normaliza y los enruta a los servicios de procesamiento y almacenamiento (Log Analytics).

3. **Análisis, correlación y almacenamiento:**

   Log Analytics permite correlacionar eventos de diferentes fuentes, identificar patrones, causas raíz y tendencias. Los datos históricos se almacenan para auditoría y análisis forense.

4. **Automatización de respuestas y flujos:**

   Logic Apps detecta condiciones críticas, ejecuta respuestas automáticas (como notificaciones, escalamiento de incidentes, creación de tickets) y orquesta la integración con otros sistemas de TI.

5. **Visualización y exploración:**

   Los usuarios autorizados acceden a dashboards y reportes personalizados, con visibilidad integral de toda la operación, facilitando la toma de decisiones y la gestión proactiva de incidentes.

6. **Seguridad y cumplimiento:**

   Todo el acceso está controlado por Azure Active Directory y registrado para auditoría, garantizando trazabilidad y cumplimiento normativo.

Justificación de la Arquitectura

- **Centralización:**

  Elimina silos de información y reduce la complejidad operativa al consolidar todas las fuentes en una única plataforma cloud.

- **Automatización:**

  Reduce tiempos de respuesta y errores humanos mediante flujos automáticos de Logic Apps.

- **Escalabilidad y resiliencia:**

  Azure permite crecer según demanda sin rediseñar la arquitectura.

- **Seguridad y cumplimiento:**

  Control de acceso, cifrado y auditoría alineados con ISO/IEC 27001:2013 y normativas colombianas.

- **Soporte a la toma de decisiones:**

  Dashboards y reportes en tiempo real para todos los perfiles operativos y de gestión.

Relación con los Objetivos y el Alcance

- Cumple con la integración de las cinco herramientas requeridas por Global Hitss.
- Responde a los objetivos de centralización, automatización, seguridad y eficiencia definidos en el alcance.
- Alinea el diseño arquitectónico con las mejores prácticas internacionales y las necesidades reales del entorno empresarial colombiano.

Conclusiones

El desarrollo del proyecto SIMAI (Sistema Integrado de Monitoreo y Análisis de Incidentes) permitió consolidar una propuesta arquitectónica robusta, realista y adaptable al entorno de Global Hitss, empresa especializada en soluciones de tecnología para empresas de telecomunicaciones y sectores corporativos. A lo largo de este trabajo se aplicaron metodologías sólidas y se realizaron análisis técnicos, económicos y operativos que permiten visualizar con claridad la viabilidad de implementación del sistema en un entorno cloud, aprovechando al máximo las herramientas de monitoreo actuales y las capacidades de Microsoft Azure.

La arquitectura diseñada, representada en el diagrama profesional presentado, logra la integración efectiva de las cinco herramientas críticas (Zabbix, Dynatrace, Grafana, Kibana y Elasticsearch) con los servicios nativos de Azure, cumpliendo con los objetivos específicos planteados al inicio del proyecto. El flujo de datos modelado desde las fuentes de monitoreo hasta la visualización unificada en Azure Workbooks y Azure Managed Grafana demuestra la viabilidad técnica de centralizar la gestión de eventos, métricas y logs en una sola plataforma cloud.

Las historias de usuario desarrolladas (HU1 a HU5) validan que el diseño responde a las necesidades reales de los diferentes perfiles operativos de Global Hitss: operadores N1, líderes de monitoreo, administradores de TI, analistas de incidentes y responsables de seguridad. La matriz de trazabilidad de requerimientos asegura que cada funcionalidad propuesta está alineada con objetivos específicos y componentes arquitectónicos concretos.

Aspectos novedosos desarrollados

Uno de los aportes más destacados del proyecto es la integración de marcos metodológicos modernos que no son comúnmente aplicados de forma conjunta en entornos operativos reales dentro de empresas como Global Hitss. En este caso, se propuso una arquitectura que cumple con los principios del Azure Well-Architected Framework, lo que asegura un enfoque equilibrado en cuanto a confiabilidad, eficiencia, costos, seguridad y excelencia operativa.

Asimismo, se aplicó el modelo Twelve-Factor App, típicamente usado en desarrollo de software, pero adaptado aquí para asegurar que los componentes del sistema SIMAI (como los servicios de monitoreo, visualización y almacenamiento de logs) se mantengan desacoplados, escalables, resilientes y fáciles de gestionar dentro de una arquitectura cloud-native. A esto se suma el uso de TOGAF + Cloud Adaptations, permitiendo estructurar la solución en capas, roles y dominios bien definidos.

Otro aspecto relevante es el enfoque automatizado y proactivo para la gestión de incidentes de nivel N1, alineado con buenas prácticas ITIL. Esto no solo mejora la eficiencia operativa, sino que también abre las puertas a una futura integración con inteligencia artificial y análisis predictivo, lo que posicionaría a Global Hitss a la vanguardia del monitoreo tecnológico en Latinoamérica.

Referencias

Akershoek, R. (2016). *IT4IT for managing the business of IT* (Van Haren Publishing, Ed.). van Haren Publishing.

AXELOS. (2019). *ITIL Foundation: ITIL 4 Edition*. TSO.

Azure logic apps documentation. (s/f). Microsoft.com. Recuperado el 7 de junio de 2025, de https://learn.microsoft.com/en-us/azure/logic-apps/

Azure Well-Architected Framework. (s/f). Microsoft.com. Recuperado el 7 de junio de 2025, de https://learn.microsoft.com/en-us/azure/architecture/framework/

Dynatrace resources. (2025, mayo 12). Dynatrace. https://www.dynatrace.com/resources/

Grafana OSS and Enterprise. (s/f). Grafana Labs. Recuperado el 7 de junio de 2025, de https://grafana.com/docs/grafana/latest/

IBM products. (s/f). Ibm.com. Recuperado el 7 de junio de 2025, de https://www.ibm.com/products/netcool-operations-insight

Iso/iec 27001:2022. (2022). ISO. https://www.iso.org/standard/27001

IT4IT™ standards. (s/f). Opengroup.org. Recuperado el 7 de junio de 2025, de https://publications.opengroup.org/standards/it4it

Koyya, K. M., & Assistant Professor, Department of Information Technology, Sasi Institute of Technology & Engineering, Tadepalligudem (Andhra Pradesh), India. (2021). Scalable architectural pattern for integrating syslog servers with Splunk. *International Journal of Recent Technology and Engineering (IJRTE)*, *10*(2), 199–202. https://doi.org/10.35940/ijrte.b6307.0710221

The Elastic Stack. (s/f). Elastic.Co. Recuperado el 7 de junio de 2025, de https://www.elastic.co/guide/en/kibana/current/index.html

TOGAF. (s/f). Www.opengroup.org. Recuperado el 7 de junio de 2025, de https://www.opengroup.org/togaf

Understand your business like never before. (2025, mayo 13).

Welcome to Dynatrace documentation — Dynatrace docs. (s/f). Dynatrace.com. Recuperado el 7 de junio de 2025, de https://www.dynatrace.com/support/help/

Wiggins, A. (s/f). *The twelve-factor app*. 12factor.net. Recuperado el 7 de junio de 2025, de https://12factor.net/

Zabbix manual. (s/f). Zabbix.com. Recuperado el 7 de junio de 2025, de https://www.zabbix.com/documentation/current/manual

(S/f-a). Servicenow.com. Recuperado el 7 de junio de 2025, de https://www.servicenow.com/products/it-operations-management.html

(S/f-b). Owasp.org. Recuperado el 7 de junio de 2025, de https://owasp.org/www-project-secure-software-development/

(S/f-c). Microsoft.com. Recuperado el 7 de junio de 2025, de https://learn.microsoft.com/en-us/azure/architecture/example-scenario/monitoring/kpi-monitoring-elasticsearch