

PROPUESTA DE OPTIMIZACIÓN Y AUTOMATIZACIÓN PARA LA GESTIÓN DE INCIDENCIAS DE BACKUP EN AZURE MEDIANTE UN MODELO BASADO EN AIOPS

Autor

Harold Jahir Bautista

Director

Jhon Alejandro Rangel

UNIVERSIDAD SANTO TOMÁS

**FACULTAD DE INGENIERÍA DE
TELECOMUNICACIONES**

**ESPECIALIZACIÓN EN GESTIÓN DE SERVICIOS DE
TECNOLOGÍAS DE LA INFORMACIÓN**

BOGOTÁ, 2025

Dedicatoria

A mis compañeros de trabajo,

Quienes día a día transforman los desafíos en oportunidades y el lugar de trabajo en un espacio de crecimiento y camaradería. Gracias por su apoyo incondicional, su paciencia durante este proceso y por ser el pilar profesional sobre el que se construyó gran parte de este proyecto.

Este logro también es suyo.

Agradecimientos

En primer lugar, deseo expresar mi más profundo agradecimiento a mi director de trabajo de grado, Jhon Alejandro Rangel, por su invaluable guía, su paciencia y su sabiduría. Sus oportunas correcciones y su constante motivación fueron fundamentales para llevar este proyecto a buen término.

A la Universidad Santo Tomás y a la Facultad de Ingeniería de Telecomunicaciones, por brindarme la oportunidad de crecer académicamente y por la excelente formación recibida en la Especialización en Gestión de Servicios de Tecnologías de la Información.

A mis compañeros de trabajo, por su colaboración, su comprensión y el excelente ambiente profesional que me permitió compaginar mis responsabilidades laborales con el desarrollo de esta monografía.

Finalmente, un agradecimiento especial a mi familia y amigos, por su amor, apoyo y aliento incondicional en cada etapa de este camino.

Índice general

Lista de Figuras	v
Lista de Tablas	vi
Acrónimos	vii
Resumen	i
Abstract	i
1. Introducción	1
1.1. Contexto General	1
1.2. Planteamiento del Problema	1
1.3. Justificación y Relevancia	2
1.4. Estructura del Documento	2
2. Problema	3
2.1. Árbol de Problemas / Qué se quiere solucionar	3
2.1.1. Análisis Detallado del Problema Central	4
2.1.2. Desglose de las Causas Raíz (Las Raíces del Árbol)	4
2.1.3. Análisis de los Efectos Directos e Indirectos (La Copa del Árbol)	6
3. Ideación de la Solución	8
3.1. Por qué se plantea ahora la solución	8
3.1.1. Sector Objetivo	8
3.1.2. Tendencias del Sector	9
3.1.3. Análisis de Mercado	10
3.2. Árbol de Objetivos	11
3.2.1. Objetivo General	12
3.2.2. Medios / Objetivos Específicos	12
3.2.3. Fines / Efectos Esperados	13
3.3. Cuál es la situación deseada	14
3.3.1. Introducción a la Situación Deseada	14
3.3.2. Propuesta de Valor	15

4. Análisis de las Alternativas Técnicas	16
4.1. Diagnóstico Interno para Apropiar las Tecnologías	16
4.1.1. Evaluación de la Madurez de Procesos ITSM	16
4.1.2. Evaluación de Competencias Técnicas (Análisis de Brecha de Ha- bilidades)	17
4.1.3. Evaluación de la Cultura Organizacional	17
4.2. Análisis del Proceso de Transformación Digital	17
4.2.1. Alternativa 1: Optimización con Herramientas Nativas de Azure	17
4.2.2. Alternativa 2: Implementación de una Plataforma de Observabi- lidad de Terceros	18
4.2.3. Alternativa 3: Adopción de una Plataforma AIOps Integral . . .	18
4.3. Matriz de Decisión	19
5. Propuesta del Modelo y Solución Tecnológica	20
5.1. Justificación de la Solución Seleccionada	20
5.2. Modelo de Implementación por Fases	20
5.2.1. Fase 1 (Meses 1-3): Fundamentos y Ganancias Rápidas	20
5.2.2. Fase 2 (Meses 4-9): Implementación y Configuración de la Plata- forma AIOps	21
5.2.3. Fase 3 (Meses 10-12+): Automatización, Optimización y Expansión	21
5.3. Arquitectura de la Solución Propuesta (Ejemplo con ServiceNow) . . .	21
5.4. Aspectos Legales y Contratación	22
5.4.1. Marco Regulatorio Colombiano: Ley Estatutaria 1581 de 2012 .	22
5.4.2. Acuerdos de Nivel de Servicio (SLA) para la Contratación . . .	22
6. Conclusiones	23
Referencias	24
Bibliografía	25

Índice de figuras

2.1. Diagrama del Árbol de Problemas.	3
3.1. Diagrama del Árbol de Objetivos.	12

Índice de cuadros

3.1. Comparativa de Plataformas Líderes de Monitoreo y AIOps	11
4.1. Matriz de Decisión de Alternativas Técnicas	19

Acrónimos

Acrónimo	Significado
AIOps	Inteligencia Artificial para Operaciones de TI (Artificial Intelligence for IT Operations)
APM	Monitorización del Rendimiento de Aplicaciones (Application Performance Monitoring)
ARG	Azure Resource Graph
BCDR	Continuidad del Negocio y Recuperación ante Desastres (Business Continuity and Disaster Recovery)
BFSI	Banca, Servicios Financieros y Seguros (Banking, Financial Services, and Insurance)
CAGR	Tasa de Crecimiento Anual Compuesta (Compound Annual Growth Rate)
CMDB	Base de Datos de Gestión de la Configuración (Configuration Management Database)
DEX	Experiencia Digital del Empleado (Digital Employee Experience)
ITIL	Biblioteca de Infraestructura de Tecnologías de la Información (Information Technology Infrastructure Library)
ITSM	Gestión de Servicios de TI (IT Service Management)
MTTR	Tiempo Medio de Resolución (Mean Time to Resolution)
OPEX	Gastos Operativos (Operational Expenditure)
RCA	Análisis de Causa Raíz (Root Cause Analysis)
RPO	Objetivo de Punto de Recuperación (Recovery Point Objective)
RTO	Objetivo de Tiempo de Recuperación (Recovery Time Objective)
SaaS	Software como Servicio (Software as a Service)
SIC	Superintendencia de Industria y Comercio
SIEM	Gestión de Eventos e Información de Seguridad (Security Information and Event Management)
SLA	Acuerdo de Nivel de Servicio (Service Level Agreement)
SLO	Objetivo de Nivel de Servicio (Service Level Objective)
VM	Máquina Virtual (Virtual Machine)

Resumen

Este trabajo aborda la problemática de la alta incidencia de reportes de fallos en los servicios de backup de Microsoft Azure, que genera ineficiencias operativas y riesgos para la continuidad del negocio. A partir de un análisis de causa-raíz (Árbol de Problemas), se identifican deficiencias en los procesos de backup, generación y gestión de reportes. Se propone una solución integral basada en la implementación de una plataforma de AIOps (Inteligencia Artificial para Operaciones de TI), alineada con las tendencias tecnológicas de 2025. Se analizan alternativas técnicas, desde la optimización de herramientas nativas de Azure hasta la adopción de plataformas de observabilidad y AIOps. La solución recomendada se enfoca en automatizar la detección, correlación, y remediación de incidencias, mejorando el Tiempo Medio de Resolución (MTTR) y liberando recursos humanos. Finalmente, se examinan los aspectos legales y contractuales, incluyendo el cumplimiento de la Ley 1581 de 2012 en Colombia y la definición de Acuerdos de Nivel de Servicio (SLAs) robustos para la contratación de servicios en la nube.

Palabras clave: Gestión de Servicios de TI, AIOps, Azure Backup, Automatización, Monitoreo Proactivo, ITSM, Ley 1581, SLA.

Resumen

This monograph addresses the problem of the high incidence of failure reports in Microsoft Azure backup services, which generates operational inefficiencies and risks to business continuity. Based on a root-cause analysis (Problem Tree), deficiencies are identified in the backup processes, report generation, and management. A comprehensive solution is proposed based on the implementation of an AIOps (Artificial Intelligence for IT Operations) platform, aligned with the technological trends for 2025. Technical alternatives are analyzed, from optimizing native Azure tools to adopting observability and AIOps platforms. The recommended solution focuses on automating the detection, correlation, and remediation of incidents, improving Mean Time to Resolution (MTTR) and freeing up human resources. Finally, legal and contractual aspects are examined, including compliance with Colombia's Law 1581 of 2012 and the definition of robust Service Level Agreements (SLAs) for contracting cloud services.

Keywords: IT Service Management, AIOps, Azure Backup, Automation, Proactive Monitoring, ITSM, Law 1581, SLA.

Capítulo 1

Introducción

1.1. Contexto General

La transformación digital ha posicionado a los servicios en la nube como el pilar fundamental de la infraestructura empresarial moderna. Plataformas como Microsoft Azure ofrecen una escalabilidad, flexibilidad y resiliencia sin precedentes, permitiendo a las organizaciones innovar a un ritmo acelerado. En este paradigma, la gestión de la continuidad del negocio y la recuperación ante desastres (BCDR) ha evolucionado de ser una póliza de seguro reactiva a una función estratégica y proactiva, esencial para la supervivencia y competitividad en el mercado. La integridad, disponibilidad y capacidad de restauración de las copias de seguridad (backups) constituyen el núcleo de cualquier estrategia BCDR robusta, siendo la última línea de defensa contra una amplia gama de amenazas, desde ciberataques y fallos de hardware hasta errores humanos.

1.2. Planteamiento del Problema

A pesar de la sofisticación y la robustez inherentes a las plataformas de nube pública, la gestión de sus operaciones a gran escala presenta desafíos significativos que pueden mermar su valor. Este trabajo de grado se centra en un problema operativo que, aunque común, posee un alto impacto en la eficiencia y el riesgo organizacional: la gestión ineficiente de un volumen elevado y constante de notificaciones de fallos en los procesos de backup de Azure. Esta situación, como se detallará en el análisis del problema, no solo consume recursos valiosos de los equipos de Tecnologías de la Información (TI), sino que también introduce riesgos latentes que pueden comprometer directamente la capacidad de la organización para cumplir con sus Objetivos de Tiempo de Recuperación (RTO) y Objetivos de Punto de Recuperación (RPO), métricas críticas para el negocio.

1.3. Justificación y Relevancia

Esta monografía se enmarca en el campo de la Especialización en Gestión de Servicios de Tecnologías de la Información (ITSM), abordando la necesidad imperativa de evolucionar los modelos de soporte de TI. El paradigma tradicional, caracterizado por una respuesta reactiva a las alertas, se ha vuelto insostenible ante la complejidad y el volumen de datos generados por los entornos de nube híbrida. La solución propuesta en este documento, fundamentada en los principios de la Inteligencia Artificial para Operaciones de TI (AIOps), no solo busca resolver el problema específico de la gestión de backups, sino que representa un cambio de paradigma hacia una gestión de servicios moderna, proactiva y automatizada. Este enfoque se alinea directamente con las principales tendencias tecnológicas que definirán la industria para 2025 y más allá, como la automatización inteligente, el soporte predictivo y la mejora de la experiencia digital del empleado (DEX).

1.4. Estructura del Documento

El presente trabajo se organiza en cinco capítulos diseñados para guiar al lector desde la definición del problema hasta la propuesta de una solución integral y validada. El primer capítulo define y desglosa la problemática utilizando la metodología del Árbol de Problemas para identificar sus causas raíz y sus efectos en la organización. El segundo capítulo se dedica a la ideación de la solución, contextualizándola a través de un análisis del sector de TI en Colombia, las tendencias tecnológicas globales y el mercado de herramientas de monitoreo y AIOps. El tercer capítulo realiza un análisis comparativo de las alternativas técnicas disponibles, evaluando tres caminos estratégicos de distinta complejidad y nivel de inversión. El cuarto capítulo detalla la propuesta de solución tecnológica final, su arquitectura y un modelo de implementación por fases, abordando además los marcos legales y de contratación indispensables para su ejecución en el contexto colombiano. Finalmente, el quinto capítulo presenta las conclusiones del estudio, sintetizando los hallazgos y ofreciendo recomendaciones estratégicas.

Capítulo 2

Problema

2.1. Árbol de Problemas / Qué se quiere solucionar

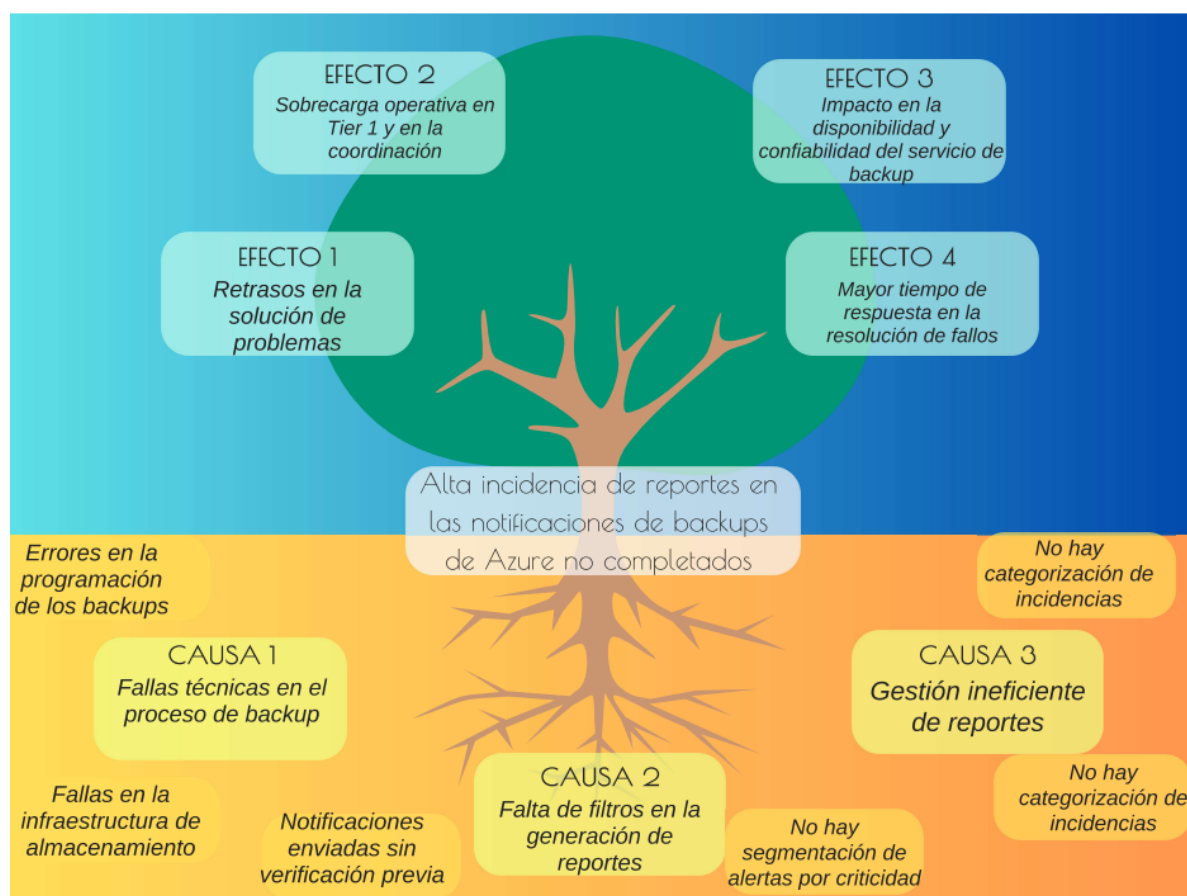


Figura 2.1: Diagrama del Árbol de Problemas.

Para comprender la magnitud y las ramificaciones del desafío operativo, se ha em-

pleado la metodología del Árbol de Problemas. Esta herramienta visual permite descomponer una situación compleja en sus componentes fundamentales: el problema central, sus causas raíz y sus efectos consecuentes. A través de este análisis, se busca ir más allá de los síntomas para identificar los factores subyacentes que deben ser abordados para lograr una solución sostenible y efectiva.

2.1.1. Análisis Detallado del Problema Central

El núcleo del desafío operativo que enfrenta la organización se define como la “Alta incidencia de reportes en las notificaciones de backups de Azure no completados”. A primera vista, esto podría interpretarse como un simple indicador de una alta tasa de fallos en las copias de seguridad. Sin embargo, un análisis más profundo revela que el problema es más sutil y pernicioso. No se trata únicamente de que los backups fallen, sino de que el sistema de notificación y alerta carece de la inteligencia necesaria para contextualizar dichos fallos. El sistema actual genera un flujo constante e indiferenciado de alertas, creando un fenómeno conocido como ruido operativo”. Este ruido ahoga las señales importantes, ya que no distingue entre fallos críticos que requieren atención inmediata, errores transitorios que se resuelven por sí solos, o falsos positivos generados por condiciones temporales. Como resultado, los equipos de soporte se ven inundados por un torrente de alertas de bajo valor, lo que degrada su capacidad de respuesta y eficiencia.

2.1.2. Desglose de las Causas Raíz (Las Raíces del Árbol)

El análisis identifica tres categorías principales de causas que contribuyen directamente al problema central. Estas causas no son exclusivamente tecnológicas, sino que también abarcan deficiencias en los procesos y en la gestión.

Causa 1: Fallas técnicas en el proceso de backup

Esta categoría agrupa los problemas técnicos directos que provocan que las tareas de copia de seguridad no se completen con éxito.

Errores en la programación de los backups: Incluye configuraciones de políticas de backup incorrectas o subóptimas. Por ejemplo, la programación de backups de alto consumo de recursos durante horas de máxima producción, la definición de ventanas de mantenimiento que entran en conflicto con otros procesos automatizados, o la aplicación de políticas genéricas que no se ajustan a los requisitos específicos de la carga de trabajo (ej. una base de datos transaccional vs. un servidor de archivos).

Fallas en la infraestructura de almacenamiento: Abarca problemas transitorios o persistentes en los servicios de almacenamiento de Azure que sustentan los backups. Esto puede incluir problemas de conectividad de red entre la máquina virtual y la

bóveda de recuperación, el agotamiento de las cuotas de almacenamiento asignadas, o fallos momentáneos en la API del servicio de almacenamiento que provocan el fracaso del trabajo de backup.

Notificaciones enviadas sin verificación previa: Este es un punto crítico que conecta la falla técnica con la ineficiencia del monitoreo. El sistema actual alerta inmediatamente después de un primer intento fallido, sin implementar una lógica de reintento automático o una breve espera para verificar si la condición del fallo fue transitoria (por ejemplo, un pico momentáneo de CPU o un error de red que se resuelve en segundos). Esta falta de un mecanismo de "debounce" o validación es una fuente principal del ruido operativo.

Causa 2: Falta de filtros en la generación de reportes

Esta causa se centra en la incapacidad del sistema de monitoreo para procesar y refinar la información antes de presentarla al equipo de operaciones.

El sistema actual opera bajo una lógica de "un evento, una alerta". Esto significa que genera un reporte o ticket por cada evento de fallo individual, sin aplicar lógicas de agrupación, correlación o supresión. Por ejemplo, un único problema de conectividad en un host de virtualización podría provocar el fallo simultáneo de los backups de 50 máquinas virtuales, generando 50 alertas idénticas en lugar de un único incidente contextualizado que señale la causa raíz común.

No hay segmentación de alertas por criticidad: Todas las alertas, independientemente del activo al que afecten, son tratadas inicialmente con la misma prioridad. Un fallo en el backup de un servidor de desarrollo sin importancia crítica genera el mismo tipo de alerta que un fallo en la copia de seguridad de la base de datos de producción que soporta el negocio. Esta falta de priorización basada en el impacto de negocio dificulta enormemente la tarea de triaje y asegura que los recursos del equipo no se asignen de manera óptima.

Causa 3: Gestión ineficiente de reportes

Esta categoría de causas se relaciona con las deficiencias en los procesos de gestión de servicios de TI (ITSM) que manejan las alertas una vez generadas.

No hay categorización de incidencias: Este es un fallo procesal fundamental. No existe un sistema robusto para clasificar las alertas entrantes según criterios como el tipo de error (ej. error de red, error de credenciales, error de agente), la criticidad del activo afectado, o el impacto potencial en el negocio. Esta carencia obliga al equipo de Nivel 1 a realizar una investigación manual desde cero para cada alerta, un proceso altamente ineficiente y repetitivo. La ausencia de esta práctica básica de Gestión de Incidentes,

un pilar de marcos como ITIL, evidencia una brecha significativa en la madurez de los procesos de la organización.

2.1.3. Análisis de los Efectos Directos e Indirectos (La Copa del Árbol)

Las causas raíz descritas anteriormente se propagan a través de la organización, generando una serie de efectos negativos que impactan la operación, el servicio y el negocio.

Efecto 1: Retrasos en la solución de problemas. El tiempo que el equipo de Nivel 1 dedica a investigar, validar y descartar alertas de bajo valor o falsos positivos es tiempo que no se dedica a resolver los problemas reales. Esta "fatiga de alertas" conduce a una desensibilización del equipo, donde las alertas importantes pueden ser pasadas por alto o atendidas con retraso, aumentando el riesgo de que un problema menor escale a una incidencia mayor.

Efecto 2: Sobrecarga operativa en Tier 1 y en la coordinación. El equipo de soporte de Nivel 1 se ve crónicamente abrumado por un alto volumen de tickets repetitivos y de baja complejidad. Esto no solo genera estrés y desmotivación, sino que también incrementa la necesidad de escalamientos y coordinación con otros equipos (redes, almacenamiento, aplicaciones) para diagnosticar problemas que podrían haberse filtrado o contextualizado desde el inicio. Esta situación representa una "deuda técnica" en el área de monitoreo y operaciones: una solución que pudo ser adecuada en sus inicios, pero que no ha escalado con el crecimiento del entorno de Azure, y ahora cobra un alto interés en forma de ineficiencia operativa.

Efecto 3: Impacto en la disponibilidad y confiabilidad del servicio de backup. Este es el riesgo de negocio más grave y la consecuencia final de las ineficiencias descritas. Mientras el equipo de operaciones está distraído por el ruido, un fallo crítico real en el backup de un sistema de misión crítica puede pasar desapercibido durante un período prolongado. Esto puede llevar a una brecha en la cadena de copias de seguridad, comprometiendo la capacidad de la organización para restaurar datos en caso de un desastre y, por lo tanto, fallando en el cumplimiento de sus RPO y RTO.

Efecto 4: Mayor tiempo de respuesta en la resolución de fallos. Como consecuencia directa y medible de los puntos anteriores, el Tiempo Medio de Resolución (MTTR), un indicador clave del rendimiento de ITSM, se ve negativamente afectado. La investigación manual, la falta de contexto y los retrasos en la detección de problemas reales se suman para alargar el ciclo de vida de los incidentes, lo que impacta directamente en los indicadores de nivel de servicio (SLIs/SLOs) y en la percepción de calidad del servicio de TI por parte del negocio. Además, la asignación constante de técnicos

cualificados a tareas repetitivas es un factor de riesgo para la retención de talento, pudiendo generar burnout y una alta rotación de personal, lo que a su vez incrementa los costos de contratación y formación.

Capítulo 3

Ideación de la Solución

Tras un análisis exhaustivo del problema, sus causas y efectos, este capítulo se dedica a la concepción de una solución estratégica. Se busca no solo corregir las deficiencias identificadas, sino proponer un modelo de gestión que sea robusto, escalable y alineado con las futuras demandas del negocio y la tecnología. Para ello, se justifica la pertinencia del proyecto en el contexto actual, se definen los objetivos claros que guiarán la implementación y se describe la visión del estado futuro deseado, articulando una propuesta de valor concreta.

3.1. Por qué se plantea ahora la solución

La decisión de abordar un problema operativo de esta naturaleza no debe ser meramente reactiva. Es fundamental justificar la inversión de tiempo, recursos y capital demostrando que las condiciones del mercado, el sector y la tecnología han alcanzado un punto de inflexión. Este es el momento oportuno para actuar porque la inacción representa un riesgo competitivo creciente, mientras que la acción se alinea con una convergencia de tendencias que hacen la solución no solo viable, sino estratégicamente necesaria.

3.1.1. Sector Objetivo

El entorno empresarial y tecnológico de Colombia proporciona un fuerte argumento para la modernización de las operaciones de TI.

Contexto de Crecimiento y Competitividad en Colombia: El sector tecnológico colombiano se encuentra en una fase de expansión acelerada. Las proyecciones indican un crecimiento del 20 % en las exportaciones del sector para el año 2025, lo que refleja un dinamismo y una capacidad de innovación crecientes. A nivel estratégico, las juntas directivas de las empresas en Colombia han redefinido sus prioridades para 2025, colocando la innovación, la tecnología y la resiliencia en la cima de su agenda para enfrentar

la volatilidad del mercado y capitalizar la transformación digital. La economía del país, aunque enfrenta desafíos macroeconómicos, muestra un crecimiento estable que es impulsado en gran medida por el sector de servicios, donde la tecnología juega un papel habilitador clave.

Implicaciones Estratégicas: En este contexto de alta competitividad, la eficiencia operativa deja de ser un objetivo secundario para convertirse en un factor crítico de diferenciación y supervivencia. Las organizaciones ya no pueden permitirse el lujo de tener a sus equipos de TI más cualificados dedicados a tareas repetitivas y de bajo valor, como la gestión de alertas de ruido. Es imperativo liberar este capital humano para que se enfoque en iniciativas de innovación que generen valor directo al negocio. La solución propuesta en esta monografía, al automatizar la gestión de incidencias de backup, se alinea perfectamente con esta prioridad estratégica, transformando un centro de costo operativo en un habilitador de agilidad.

3.1.2. Tendencias del Sector

La propuesta no surge en un vacío tecnológico, sino que se apoya en un conjunto de macro tendencias globales que validan su enfoque y confirman su pertinencia a largo plazo.

La Era de la Automatización Inteligente y el Soporte Proactivo: Las previsiones para 2025 en el ámbito del soporte y la gestión de servicios de TI apuntan de manera inequívoca hacia un futuro dominado por la automatización inteligente y el soporte proactivo y predictivo. La industria está migrando de un modelo donde los humanos reaccionan a problemas, a uno donde la Inteligencia Artificial (IA) y el Aprendizaje Automático (Machine Learning) se encargan de analizar datos, detectar patrones, predecir fallos y ejecutar tareas repetitivas, permitiendo que los equipos humanos se concentren en la resolución de problemas complejos y en la estrategia.

Tendencias Tecnológicas Estratégicas de Gartner para 2025: El análisis de Gartner refuerza esta visión. Tendencias como la IA Agéntica, que describe equipos virtuales de agentes de IA que asisten y complementan el trabajo humano, y las Plataformas de Gobernanza de IA, que permiten gestionar el ciclo de vida de estos sistemas de forma responsable, son centrales para el futuro de las operaciones. La solución propuesta es una manifestación práctica de estas tendencias, buscando crear un .agente de IA. especializado en la gestión de alertas de backup.

AIOps como Paradigma Central: El concepto de AIOps se ha consolidado como la tendencia principal para la gestión de operaciones de TI modernas. Su propósito es utilizar análisis avanzados y machine learning sobre los datos de telemetría (logs, métricas, trazas) para anticiparse a los problemas antes de que afecten a los usuarios. Las

plataformas AIOps están diseñadas específicamente para analizar grandes volúmenes de datos, identificar patrones significativos y habilitar respuestas proactivas y automatizadas, abordando directamente la complejidad y el ruido”de los entornos de TI actuales.

3.1.3. Análisis de Mercado

El mercado de herramientas de monitoreo y AIOps no solo respalda estas tendencias, sino que demuestra una fuerte validación comercial y una trayectoria de crecimiento robusta.

Crecimiento Exponencial del Mercado AIOps: El mercado global de AIOps está experimentando un crecimiento notable. Las proyecciones de mercado indican que el tamaño del mercado crecerá desde aproximadamente 11.16 mil millones de dólares en 2025 hasta más de 32 mil millones de dólares para 2029, con una Tasa de Crecimiento Anual Compuesta (CAGR) que se sitúa consistentemente por encima del 25 % en diversos informes. Otros análisis proyectan un CAGR igualmente fuerte, entre el 17 % y el 19.4 % a más largo plazo. Este dinamismo del mercado indica una alta demanda y una adopción acelerada de estas tecnologías por parte de las empresas, lo que reduce el riesgo de inversión en una solución de este tipo.

Segmentación y Adopción del Mercado: El mercado de AIOps está segmentado por múltiples vectores. Por tamaño de organización, las grandes empresas son las principales adoptantes, impulsando la demanda debido a la complejidad de sus infraestructuras de TI. Por modo de despliegue, aunque las soluciones on-premise todavía mantienen una cuota importante por razones de regulación y seguridad en sectores como el financiero, el segmento de despliegue en la nube (SaaS) es el que crece a un ritmo más rápido. Los sectores de Banca, Servicios Financieros y Seguros (BFSI) y de TI y Telecomunicaciones son los líderes en la implementación de AIOps.

Principales Jugadores del Mercado: El ecosistema de proveedores es maduro y competitivo. Incluye a gigantes tecnológicos establecidos como Splunk, IBM, BMC Software, Cisco (a través de AppDynamics) y ServiceNow, que han incorporado capacidades de AIOps en sus plataformas de gestión y monitoreo. Junto a ellos, existen especialistas en observabilidad y AIOps que han ganado una tracción significativa, como Datadog, Dynatrace, Moogsoft y BigPanda. Estos proveedores son consistentemente reconocidos como líderes en los análisis de firmas de prestigio como Gartner y Forrester, lo que proporciona una base sólida para la evaluación y selección de herramientas. La siguiente tabla resume las características de algunos de los actores más relevantes.

Cuadro 3.1: Comparativa de Plataformas Líderes de Monitoreo y AIOps

Plataforma	Enfoque Principal	Fortalezas Clave	Debilidades / Consideraciones
Datadog	Observabilidad Cloud-Native	Facilidad de uso, dashboards intuitivos, +600 integraciones, monitoreo en tiempo real.	Costo puede escalar con volumen de datos. Integración nativa y profunda con Azure.
Splunk	Gestión de Logs y Seguridad (SIEM)	Potente lenguaje de búsqueda (SPL), alta personalización, líder en análisis de logs, opciones on-premise.	Curva de aprendizaje pronunciada, puede ser costoso, menos intuitivo para monitoreo de infra. en tiempo real. Fuerte integración con Azure mediante Add-on.
ServiceNow	Plataforma de Flujos de Trabajo (ITSM/ITOM)	Integración nativa con CMDB/ITSM, automatización de flujos de remediación, enfoque en ciclo de vida del incidente.	Complejo y costoso; requiere madurez en procesos ITSM. Integración de alto rendimiento con Azure Resource Graph.
Dynatrace	Observabilidad Full-Stack y AIOps	Motor de IA (Davis) para RCA automatizado, mapeo de dependencias en tiempo real (Smartscape).	Solución premium, puede ser sobreinversión para casos simples. Sólida integración con Azure para APM y anomalías.

3.2. Árbol de Objetivos

Partiendo de la estructura del Árbol de Problemas, el Árbol de Objetivos traduce cada elemento negativo en un estado positivo deseado. Esta metodología transforma las causas en medios y los efectos en fines, proporcionando una hoja de ruta clara y lógica para la solución.

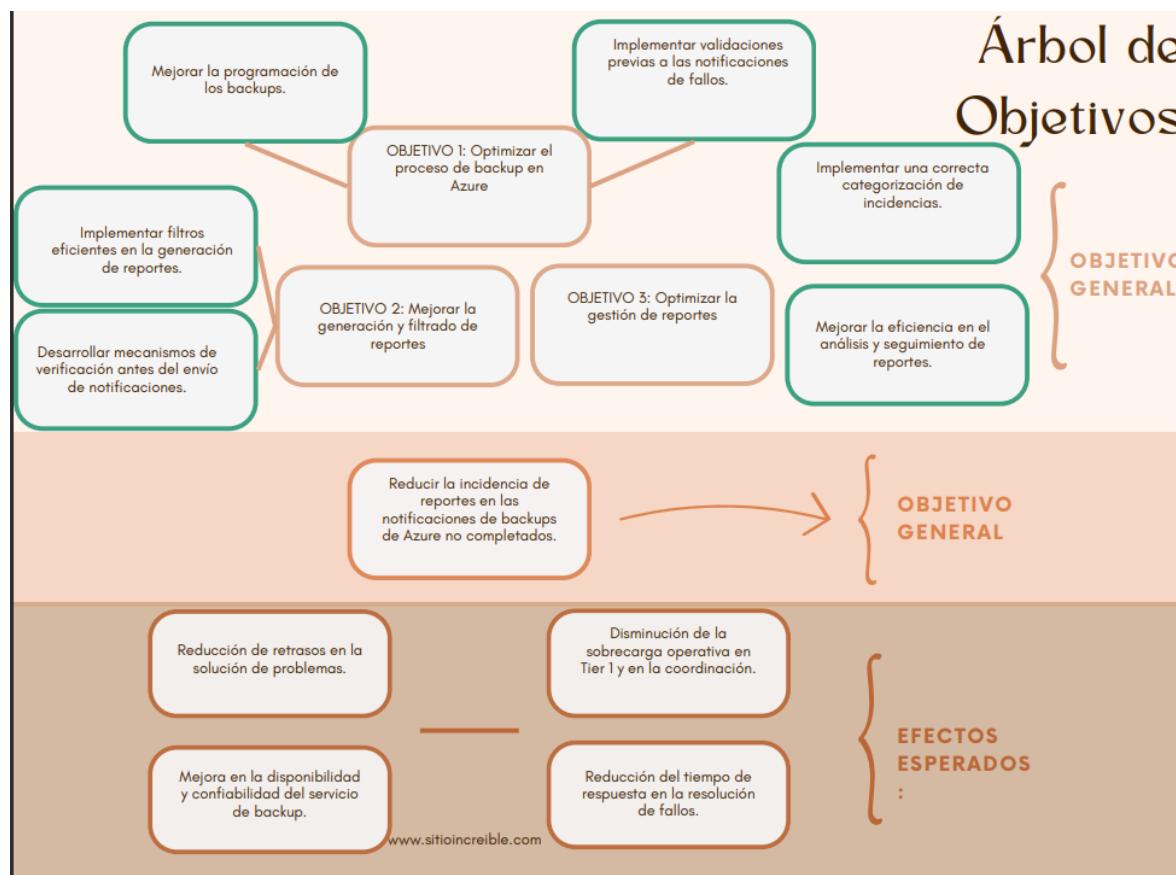


Figura 3.1: Diagrama del Árbol de Objetivos.

3.2.1. Objetivo General

El objetivo principal y estratégico del proyecto es “Reducir la incidencia de reportes en las notificaciones de backups de Azure no completados”. Este objetivo va más allá de una simple reducción numérica; busca una transformación cualitativa del proceso. El fin último es convertir el sistema de monitoreo de backups de un generador de ruido, reactivo y laborioso, a un sistema inteligente, silencioso, proactivo y, en gran medida, autónomo.

3.2.2. Medios / Objetivos Específicos

Para alcanzar el objetivo general, es necesario abordar las causas raíz del problema a través de tres objetivos específicos, que actúan como los pilares de la solución:

Objetivo 1: Optimizar el proceso de backup en Azure. Este objetivo ataca directamente la Causa 1: Fallas técnicas”. Las acciones clave para lograrlo son:

- Mejorar la programación de los backups: Revisar y optimizar las políticas de

backup existentes para alinearlas con las mejores prácticas y los requisitos de cada carga de trabajo.

- Implementar validaciones previas a las notificaciones de fallos: Desarrollar una lógica de reintentos automáticos y de verificación para filtrar los errores transitorios en la fuente, antes de que se genere una alerta.

Objetivo 2: Mejorar la generación y filtrado de reportes. Este objetivo se enfoca en resolver la Causa 2: Falta de filtros”. Las acciones necesarias son:

- Implementar filtros eficientes en la generación de reportes: Introducir mecanismos de correlación de eventos para agrupar alertas relacionadas y suprimir duplicados.
- Desarrollar mecanismos de verificación antes del envío de notificaciones: Similar a la acción del Objetivo 1, pero enfocado en la capa de procesamiento de eventos, asegurando que solo las alertas persistentes y validadas se conviertan en notificaciones.

Objetivo 3: Optimizar la gestión de reportes. Este objetivo aborda directamente la Causa 3: Gestión ineficiente se centra en mejorar los procesos de ITSM. Las acciones son:

- Implementar una correcta categorización de incidencias: Establecer un esquema de clasificación automática de alertas basado en la criticidad del activo, el tipo de error y el impacto de negocio.
- Mejorar la eficiencia en el análisis y seguimiento de reportes: Automatizar el enriquecimiento de las alertas con datos de contexto (logs, métricas de rendimiento, información de la CMDB) para acelerar el diagnóstico.

3.2.3. Fines / Efectos Esperados

La consecución exitosa de estos objetivos se traducirá directamente en la reversión de los efectos negativos identificados en el Árbol de Problemas, generando un valor tangible para la organización:

- Reducción de retrasos en la solución de problemas: Al eliminar el ruido y proporcionar contexto, los problemas reales se identifican y resuelven más rápidamente.
- Disminución de la sobrecarga operativa en Nivel 1: La automatización del triaje y la gestión de alertas de bajo valor libera al equipo para tareas más estratégicas.
- Mejora en la disponibilidad y confiabilidad del servicio de backup: Un enfoque proactivo en los fallos críticos asegura la integridad de la estrategia BCDR y el cumplimiento de los RPO/RTO.

- Reducción del tiempo de respuesta en la resolución de fallos: Una mejora medible en el MTTR, lo que impacta positivamente en los SLAs y en la percepción de la calidad del servicio de TI.

3.3. Cuál es la situación deseada

La visión final del proyecto es la creación de un ecosistema de gestión de operaciones de TI resiliente, inteligente y eficiente. Este estado futuro representa un cambio fundamental en la forma en que el equipo de TI interactúa con sus sistemas de monitoreo.

3.3.1. Introducción a la Situación Deseada

En el estado futuro, el equipo de operaciones de TI deja de ser un receptor pasivo de un flujo interminable de alertas para convertirse en un supervisor estratégico de un sistema automatizado. Este sistema ideal exhibe las siguientes capacidades:

- **Correlación Inteligente de Eventos:** Es capaz de ingerir cientos de alertas individuales de fallo de backup, reconocer que todas fueron causadas por un único evento subyacente (como la saturación de un enlace de red o un fallo en una API de almacenamiento), y consolidarlas en un único incidente inteligente y contextualizado.
- **Supresión de Ruido y Auto-remediación:** Ignora y suprime automáticamente los fallos transitorios que se resuelven por sí solos en un segundo intento programado, sin generar ninguna notificación. Esto elimina una fuente importante de "fatiga de alertas".
- **Priorización Basada en el Impacto de Negocio:** Utiliza la información de una CMDB para priorizar automáticamente las alertas. Un fallo en el backup de una base de datos de producción crítica se eleva inmediatamente a la máxima prioridad con notificaciones urgentes, mientras que fallos en entornos de desarrollo o pre-producción se registran con una prioridad más baja o se manejan de forma totalmente automatizada.
- **Remediación Guiada o Automatizada:** Para patrones de fallo conocidos y recurrentes (por ejemplo, una bóveda de recuperación que se acerca a su límite de cuota), el sistema no solo alerta, sino que puede iniciar acciones proactivas. Podría crear automáticamente un ticket en el sistema de ITSM con la solución recomendada, o incluso ejecutar un runbook de automatización para, por ejemplo, solicitar la ampliación del almacenamiento, previa aprobación. Este enfoque se aleja del monitoreo tradicional y se adentra en el campo de la observabilidad, que no solo pregunta "¿está el sistema funcionando?", sino que proporciona el contexto necesario para entender el "porqué" de un fallo.

3.3.2. Propuesta de Valor

La transición hacia este estado deseado genera una propuesta de valor multifacética que impacta positivamente en las finanzas, las operaciones, el riesgo y el talento humano.

- **Reducción de Gastos Operativos (OPEX):** El beneficio más directo es la drástica disminución de las horas-hombre dedicadas a la gestión manual de incidentes de bajo valor. Estudios de la industria indican que la implementación de AIOps puede reducir la carga de trabajo de triaje manual hasta en un 61 % y los costos operativos generales de TI hasta en un 30 %.
- **Mejora del Cumplimiento de SLAs y Mitigación de Riesgos:** Al reducir significativamente el MTTR (con mejoras promedio que oscilan entre el 30 % y el 42 % o más) y asegurar que los fallos críticos se aborden de manera prioritaria, la organización minimiza el riesgo de pérdida de datos. Esto garantiza un cumplimiento más robusto de los RPO y RTO, fortaleciendo la postura de continuidad del negocio y reduciendo el riesgo de penalizaciones contractuales o daños a la reputación.
- **Aumento de la Productividad y Enfoque en la Innovación:** La automatización de tareas operativas repetitivas libera al personal técnico cualificado. Este capital humano puede ser reasignado a proyectos estratégicos de mayor valor, como la optimización de la arquitectura en la nube, el desarrollo de nuevas aplicaciones o la mejora de los servicios al cliente, impulsando así la agenda de transformación digital de la empresa.
- **Mejora en la Experiencia del Empleado (EX) y Retención de Talento:** Al eliminar la "fatiga de alertas" y el burnout asociados con el trabajo repetitivo y de alta presión, se mejora significativamente la satisfacción laboral del equipo de operaciones de TI. Un entorno de trabajo más estimulante y menos reactivo contribuye a una mayor retención de talento, reduciendo los costos y la interrupción asociados con la alta rotación de personal.

Capítulo 4

Análisis de las Alternativas Técnicas

La transición desde el estado actual, reactivo y ruidoso, hacia la situación deseada, proactiva e inteligente, puede lograrse a través de diferentes caminos tecnológicos. No existe una única solución universal; la elección óptima depende de una combinación de factores que incluyen la madurez organizacional, las capacidades técnicas existentes, las restricciones presupuestarias y el apetito por la transformación. Este capítulo analiza tres alternativas estratégicas, presentadas como un continuo de madurez, y proporciona un marco para que la organización evalúe su propia preparación antes de embarcarse en este proceso de cambio.

4.1. Diagnóstico Interno para Apropiar las Tecnologías

Antes de evaluar las soluciones externas, es imperativo que la organización realice un diagnóstico interno honesto y exhaustivo. Este proceso de autoevaluación es un componente crítico de la gestión del cambio y determinará en gran medida el éxito de la implementación de cualquiera de las alternativas. Una monografía enfocada en la gestión de servicios de TI debe enfatizar que la tecnología por sí sola no resuelve problemas procesales o culturales.

4.1.1. Evaluación de la Madurez de Procesos ITSM

El primer pilar del diagnóstico es evaluar la madurez de los procesos de ITSM existentes, basados en marcos como ITIL. Se deben plantear preguntas clave: ¿Existe un proceso formal y documentado para la Gestión de Incidentes, la Gestión de Problemas y la Gestión de Cambios? ¿Se utiliza y mantiene una Base de Datos de Gestión de la Configuración (CMDB) que refleje con precisión el entorno de TI? Una organización con una baja madurez en estos procesos fundamentales encontrará enormes dificultades

para implementar y obtener valor de una solución AIOps avanzada como ServiceNow, que depende intrínsecamente de estos procesos para funcionar correctamente.

4.1.2. Evaluación de Competencias Técnicas (Análisis de Brecha de Habilidades)

El segundo pilar es evaluar el capital humano. ¿El equipo actual posee las habilidades necesarias para implementar y gestionar la solución elegida? Esto incluye competencias en scripting (particularmente PowerShell para el entorno Azure), conocimiento de APIs REST, fundamentos de análisis de datos y, para las soluciones más avanzadas, conceptos de Machine Learning. La escasez de talento con conocimientos específicos en AIOps es una barrera de adopción reconocida globalmente. La decisión entre las alternativas dependerá de un balance realista entre las capacidades internas, la capacidad de la organización para capacitar a su personal y su disposición para contratar nuevos talentos o apoyarse en servicios de consultoría externa.

4.1.3. Evaluación de la Cultura Organizacional

El tercer pilar, y a menudo el más desafiante, es la cultura. ¿Existe una cultura que fomente la automatización y la colaboración interdepartamental, como en los modelos DevOps? ¿O la organización está caracterizada por silos funcionales (redes, servidores, seguridad) y una resistencia generalizada al cambio? La implementación de una plataforma de AIOps no es simplemente un proyecto tecnológico; es un proyecto de transformación cultural. Requiere el patrocinio activo de la alta dirección, la colaboración estrecha entre equipos y la voluntad de redefinir roles y responsabilidades. Sin este respaldo cultural, incluso la mejor tecnología está destinada a fracasar.

4.2. Análisis del Proceso de Transformación Digital

Una vez completado el diagnóstico interno, la organización puede evaluar de manera informada las siguientes tres alternativas, que representan caminos evolutivos hacia la solución del problema.

4.2.1. Alternativa 1: Optimización con Herramientas Nativas de Azure

Descripción: Esta alternativa se centra en maximizar el valor y la funcionalidad de las herramientas que ya están disponibles dentro de la suscripción de Microsoft Azure. Representa el enfoque de menor costo de adquisición inicial y la curva de aprendizaje más suave.

Componentes Técnicos Clave:

- Implementación de Mejores Prácticas de Azure Backup.
- Automatización con Azure Automation Runbooks y PowerShell.
- Gobernanza a Escala con Azure Policy.
- Análisis Centralizado con Azure Resource Graph (ARG).

Ventajas: Bajo costo de adquisición, utiliza un conjunto de herramientas ya conocido, implementación rápida.

Desventajas: Nivel de automatización e inteligencia limitado, no resuelve correlación de eventos complejos, enfoque mayormente reactivo.

4.2.2. Alternativa 2: Implementación de una Plataforma de Observabilidad de Terceros

Descripción: Introduce una plataforma especializada de un tercero para agregar, analizar y visualizar datos de telemetría de todo el entorno de TI, no solo de Azure.

Componentes Técnicos Clave:

- Ingesta Centralizada de Datos (logs, métricas, trazas).
- Dashboards y Visualización Avanzada (ej. Datadog, Splunk).
- Alertas Inteligentes y Basadas en Machine Learning.
- Análisis Profundo de Logs y Causa Raíz.

Ventajas: Visibilidad centralizada, capacidades de alerta y análisis superiores, sienta las bases para AIOps.

Desventajas: Costo de licenciamiento significativo, requiere aprendizaje de nueva herramienta, la remediación no es su función principal.

4.2.3. Alternativa 3: Adopción de una Plataforma AIOps Integral

Descripción: El enfoque más avanzado. Utiliza IA para entender relaciones causales, predecir problemas y automatizar la respuesta, integrando monitoreo con flujos de ITSM.

Componentes Técnicos Clave:

- Correlación de Eventos y Reducción de Ruido automatizada.
- Análisis de Causa Raíz (RCA) Automatizado (ej. ServiceNow, Dynatrace).
- Remediación Guiada y Automatizada.
- Integración Nativa con ITSM y CMDB.

Ventajas: Máximo nivel de automatización, reducción drástica de MTTR, transición a modelo proactivo y predictivo.

Desventajas: Mayor costo y complejidad, requiere alta madurez organizacional, riesgo de dependencia de un proveedor.

4.3. Matriz de Decisión

Cuadro 4.1: Matriz de Decisión de Alternativas Técnicas

Criterio de Evaluación	Alt. 1: Azure Nativo	Alt. 2: Observabilidad	Alt. 3: AIOps Integral	Ponderación
Costo Estimado (TCO 3 años)	Bajo (OPEX de personal)	Medio (Licencias + OPEX)	Alto (Licencias + Implementación)	20 %
Complejidad de Implementación	Baja	Media	Alta	15 %
Nivel de Automatización	Bajo (Scripts puntuales)	Medio (Alertas inteligentes)	Alto (Correlación, RCA, remediación)	25 %
Impacto en Reducción de MTTR	Bajo (10-15 %)	Medio (30-40 %)	Alto (>50 %)	25 %
Requisitos de Madurez Org.	Bajos (Conocimientos Azure)	Medios (Procesos monitoreo)	Altos (Procesos ITSM, CMDB)	15 %

Capítulo 5

Propuesta del Modelo y Solución Tecnológica

Tras el análisis comparativo, este capítulo detalla la solución recomendada, su arquitectura, un plan de implementación pragmático y los marcos legales y contractuales que gobiernan su ejecución.

5.1. Justificación de la Solución Seleccionada

Se recomienda la adopción de la **Alternativa 3: Adopción de una Plataforma AIOps Integral**. Aunque representa la mayor inversión, es la única que aborda de manera fundamental todas las causas raíz del problema. Su capacidad para automatizar la correlación, el análisis de causa raíz y la remediación ofrece el mayor impacto en la reducción del MTTR y la carga operativa. Es una inversión en la capacidad competitiva futura de la organización.

5.2. Modelo de Implementación por Fases

Se propone un modelo de negocio interno basado en una implementación por fases para gestionar el riesgo y demostrar valor incrementalmente.

5.2.1. Fase 1 (Meses 1-3): Fundamentos y Ganancias Rápidas

- **Objetivo:** Limpiar el ruido.^{en} la fuente y establecer una base de datos sólida.
- **Acciones:** Implementar componentes clave de la Alternativa 1 (optimizar políticas de Azure Backup, centralizar logs en Log Analytics, usar Azure Policy).
- **Entregable:** Entorno de Azure Backup estandarizado y datos listos para AIOps.

5.2.2. Fase 2 (Meses 4-9): Implementación y Configuración de la Plataforma AIOps

- **Objetivo:** Desplegar la plataforma AIOps (ej. ServiceNow ITOM) y establecer visibilidad.
- **Acciones:** Adquirir plataforma, conectarla a Azure (Log Analytics, Resource Graph), poblar CMDB, configurar dashboards y reglas de correlación básicas.
- **Entregable:** Plataforma AIOps operativa con visibilidad centralizada y reducción inicial de ruido.

5.2.3. Fase 3 (Meses 10-12+): Automatización, Optimización y Expansión

- **Objetivo:** Evolucionar de la detección a la remediación y predicción.
- **Acciones:** Desarrollar runbooks de remediación, integrar con ChatOps, entrenar modelos de Machine Learning, explorar casos de uso predictivos.
- **Entregable:** Sistema de gestión de incidentes altamente automatizado y expandible a otras áreas de TI.

5.3. Arquitectura de la Solución Propuesta (Ejemplo con ServiceNow)

La arquitectura se diseña como un sistema de múltiples capas:

1. **Capa de Fuentes de Datos (Azure):** VMs, Storage, Bóvedas de Recuperación.
2. **Capa de Agregación (Azure Monitor):** Log Analytics Workspace y Azure Resource Graph.
3. **Capa de Ingesta y Procesamiento (Conector ServiceNow):** Conector oficial para Azure ITOM que normaliza y asocia datos con CIs en la CMDB.
4. **Capa de Inteligencia (Motor AIOps de ServiceNow):** Aplica Machine Learning para correlacionar eventos, detectar anomalías, analizar causa raíz y suprimir ruido.
5. **Capa de Acción y Flujo de Trabajo (ServiceNow ITSM y Automatización):** Crea y gestiona tickets de incidentes, e invoca flujos de trabajo de remediación automatizada a través de Azure Automation.

5.4. Aspectos Legales y Contratación

La adopción de una solución SaaS requiere un análisis riguroso del marco legal colombiano y la definición de acuerdos contractuales robustos.

5.4.1. Marco Regulatorio Colombiano: Ley Estatutaria 1581 de 2012

Esta ley establece el régimen general de protección de datos personales. Al usar una plataforma AIOps en la nube, se deben definir roles:

- **Responsable del Tratamiento:** La empresa que contrata el servicio. Es dueña de los datos y define la finalidad de su tratamiento.
- **Encargado del Tratamiento:** El proveedor de la plataforma AIOps (ej. ServiceNow). Procesa los datos por cuenta del Responsable.

La relación debe estar mediada por un **contrato de transmisión de datos** que estipule las obligaciones del Encargado. Además, se debe cumplir con el principio de **responsabilidad demostrada (Accountability)**, realizando evaluaciones de impacto y adoptando enfoques de "Privacidad desde el Diseño".

5.4.2. Acuerdos de Nivel de Servicio (SLA) para la Contratación

El SLA es la herramienta de gobernanza fundamental. Debe incluir:

- Descripción detallada de los servicios.
- Métricas de rendimiento y Objetivos de Nivel de Servicio (SLOs): Disponibilidad, rendimiento, gestionabilidad.
- Compromisos de seguridad y cumplimiento con la Ley 1581.
- Soporte técnico y tiempos de respuesta garantizados.
- Penalizaciones por incumplimiento.
- Proceso de terminación y estrategia de salida segura de los datos.

Capítulo 6

Conclusiones

Al finalizar este exhaustivo análisis, se pueden extraer una serie de conclusiones fundamentales que no solo validan la solución propuesta, sino que también ofrecen una perspectiva estratégica sobre la evolución de la gestión de servicios de TI.

Síntesis del Problema y la Solución: Se ha demostrado que el problema central de la .alta incidencia de reportes.^{es} el resultado de una brecha sistémica en la madurez de los procesos de monitoreo. La solución propuesta, basada en AIOps, aborda sistemáticamente cada causa raíz, proponiendo un cambio de paradigma desde la reacción manual hacia la automatización proactiva.

Validación de la Propuesta como Respuesta Estratégica: La adopción de AIOps se confirma como una respuesta estratégica y oportuna, alineada con las tendencias tecnológicas, con un retorno de la inversión tangible (mejora de MTTR, reducción de OPEX) y con la capacidad de mitigar riesgos de negocio críticos.

Importancia del Enfoque Holístico y la Madurez Organizacional: El éxito de una iniciativa de AIOps no reside exclusivamente en la tecnología. Depende de un enfoque holístico que considere procesos de ITSM maduros, competencias técnicas, gestión del cambio cultural y una gobernanza rigurosa. El modelo de implementación por fases permite que la tecnología y la organización maduren en paralelo.

Reflexión Final sobre el Futuro de la Gestión de Servicios de TI: La transición hacia operaciones de TI impulsadas por IA es una necesidad competitiva presente. Este trabajo ilustra el camino práctico y estratégico para iniciar esta transformación. Al automatizar lo predecible, se libera el potencial humano para que se enfoque en lo excepcional. La implementación de AIOps es el primer paso hacia un futuro de operaciones de TI autónomas, predictivas y alineadas con la velocidad del negocio.

Referencias

Bibliografía

- [1] COS Global Services. (2025). *Top 5 tendencias en soporte IT para 2025*.
- [2] Alvarez, G. (2024). *Las 10 principales tendencias tecnológicas estratégicas de Gartner para 2025*. Gartner.
- [3] Deel. (s.f.). *Tendencias de IT para 2025*.
- [4] EY. (2025). *Tendencias tecnológicas 2025: Colombia, camino hacia la innovación*.
- [5] Sectorial. (2025). *Se proyecta un crecimiento del 20 % en las exportaciones del sector tecnológico en 2025*.
- [6] BBVA Research. (2025). *Colombia: de las grandes tendencias al desempeño de los sectores*.
- [7] Gartner. (2025). *The Top AI Trends for 2025*.
- [8] Motadata. (s.f.). *AIOps Trends 2025: Innovation in IT Management*.
- [9] Gartner. (s.f.). *AIOps Platforms Reviews and Ratings*.
- [10] Hewitt, P. (s.f.). *Gartner: Top Trends Impacting Infrastructure and Operations for 2025*. APMdigest.
- [11] Site24x7. (2025). *Top AWS monitoring trends in 2025*.
- [12] IT Convergence. (s.f.). *Top Strategic Cloud Computing Predictions for 2025 and Onwards*.
- [13] Lei, A. (2025). *Azure Backup and Recovery Best Practices for 2025*. BytePlus.
- [14] AIS. (2024). *Data Backup Best Practices 2024*.
- [15] CloudAlly. (2025). *Top 8 Microsoft 365 Backup Best Practices for 2025*.
- [16] Microsoft Learn. (2025). *Recommended configuration options for Azure Backup*.
- [17] Función Pública. (2012). *Ley 1581 de 2012*.

-
- [18] Departamento Nacional de Planeación. (s.f.). *Guía normativa para la explotación de datos*.
 - [19] Red Iberoamericana de Protección de Datos. (2021). *Recomendaciones sobre el tratamiento de datos personales en servicios de computación en la nube*.
 - [20] Forrester. (2025). *The Forrester Wave™: AIOps Platforms, Q2 2025*.
 - [21] Dynatrace. (s.f.). *Forrester AIOps Wave Report*.
 - [22] Microsoft Azure Blog. (s.f.). *Azure Resource Graph unlocks enhanced discovery for ServiceNow*.
 - [23] Microsoft. (2025). *Service Level Agreements (SLA) for Online Services*.