Modelo Cloud Híbrido para la Innovación y Gestión Eficiente: Caso de Estudio en Anónima SA

Miguel Fernando Gómez Alfonso

John Alexander Peña Ortiz

Docente

Andrés Felipe Guarnizo Saavedra

Universidad EAN

Unidad de estudio: Seminario de Investigación Especialización

Especialización en Gerencia de Tecnología

2024

Contenido

Índice de Tablas e Ilustraciones

Resumen

Este informe examina los retos de **Anónima S.A.** en la adopción de la nube bajo el **Modelos (CAF)**, centrándose en la integración de sus plataformas tecnológicas con un enfoque estructurado. Para abordar esta problemática, se adopta un enfoque cualitativo con un diseño de investigación no experimental, transversal y descriptivo, basado en fuentes secundarias.

La metodología emplea técnicas de **Design Thinking**, aplicando el **Diagrama de Causa y Efecto (Ishikawa)** en las fases de **Empatía y Definición** para identificar barreras y oportunidades en la adopción de la nube. Posteriormente, se utiliza **Lluvia de Ideas** en la fase de **Ideación** para generar soluciones innovadoras alineadas con las seis perspectivas del CAF. En la fase de **Prototipado**, se desarrollan **Prototipos de Imagen** para visualizar las soluciones propuestas y una **Matriz RACI** para definir responsabilidades en la implementación del modelo de adopción.

Los resultados contribuirán a diseñar un marco de adopción de la nube eficiente, asegurando la alineación con las mejores prácticas del sector y optimizando la integración de entornos híbridos en la gestión de TI.

Palabras clave: CAF, adopción de la nube, Design Thinking, Diagrama de Ishikawa, Lluvia de Ideas, Prototipos de Imagen, Matriz RACI.

Planteamiento del Problema

Descripción del problema

El origen del problema radica en que Anónima SA tiene un modelo de operación de TI interno basado en silos. Esto significa que las diferentes áreas de la organización operan de manera aislada, sin una integración efectiva entre sus procesos y sistemas. Este enfoque fragmentado dificulta la alineación con las filosofías y servicios de las nubes públicas, lo que limita la capacidad de la organización para aprovechar las oportunidades que ofrecen las tecnologías modernas.

Los síntomas de este problema se manifiestan en ineficiencias operativas, como retrasos en la implementación de nuevas soluciones, duplicidad de esfuerzos y dificultades para responder rápidamente a las necesidades cambiantes del negocio. Además, la falta de un modelo unificado genera costos elevados debido al uso ineficiente de los recursos disponibles y a la necesidad de mantener infraestructuras redundantes.

Para Anónima S.A., operar las plataformas de cloud públicas con un modelo tradicional por silos conlleva riesgos significativos, como altos costos operativos, ineficiencia en la gestión de recursos y una limitada eficacia para responder a las demandas del mercado. Además, este enfoque incrementa las vulnerabilidades en materia de seguridad y dificulta la implementación de estrategias de innovación tecnológica, afectando la competitividad y la capacidad de adaptación de la organización.

El abordaje efectivo de esta problemática radica en el diseño e implementación de un modelo operativo de cloud híbrido que permita a Anónima S.A. integrar de manera eficiente sus entornos on-premises y nubes públicas. Este modelo optimizará el uso de recursos, fortalecerá la seguridad, fomentará la colaboración entre las áreas de TI y aumentará la eficiencia y agilidad organizacional.

Pregunta de investigación

¿Cuál es el enfoque más adecuado para diseñar un modelo operativo ágil y eficiente que permita a Anónima S.A. integrar sus entornos on-premises y nubes públicas, optimizando su área de TI interna?

Objetivos

Objetivo general

Diseñar un modelo operativo que permita a Anónima SA gestionar de manera eficiente su área de TI interna, integrando subscripciones en nubes públicas con sistemas on-premises bajo un enfoque ágil y escalable.

Objetivos específicos

1. Analizar las limitaciones del modelo de operación de TI interno basado en silos frente a los requerimientos de entornos híbridos.
2. Identificar las mejores prácticas y marcos de trabajo para la administración de subscripciones en nubes públicas y su integración con los sistemas internos.
3. Proponer un nuevo modelo de organización fundacional que integre las capacidades del modelo actual con el diseño del modelo operativo cloud propuesto.

Marco Teórico

El marco teórico establece los fundamentos conceptuales y metodológicos para abordar la problemática del modelo operativo cloud híbrido en Anónima SA. A través de un análisis exhaustivo de enfoques y teorías clave, se busca proporcionar una base sólida que permita entender, diseñar e implementar estrategias óptimas en este ámbito.

TOE Framework (Technology-Organization-Environment)

El modelo TOE (Technology-Organization-Environment) es un marco conceptual esencial para analizar y guiar la adopción y operación de tecnologías en un entorno cloud. Este enfoque permite identificar los factores clave que deben considerarse para implementar y operar eficazmente un modelo cloud híbrido, asegurando una integración exitosa entre sistemas on-premises y en la nube. Las tres dimensiones del TOE Framework aplicadas específicamente a la operación cloud son las siguientes:

Dimensión Tecnológica:

La dimensión tecnológica analiza las capacidades y requisitos técnicos necesarios para operar una infraestructura cloud hibrida. Esto incluye la compatibilidad entre plataformas, la escalabilidad de los recursos y la capacidad de integración de herramientas de monitoreo y gestión.

Para optimizar la operación cloud, se debe implementar una arquitectura que soporte la automatización de procesos, el balanceo dinámico de cargas de trabajo y el uso de contenedores o virtualización para maximizar la flexibilidad.

Es fundamental garantizar que las plataformas tecnológicas sean interoperables mediante el uso de APIs abiertas y middleware avanzado que facilite el intercambio de datos y procesos entre entornos locales y la nube pública.

Dimensión Organizacional:

Esta dimensión considera la preparación interna de la organización para operar en un modelo cloud. Es esencial definir roles y responsabilidades claros dentro del equipo de TI para gestionar tanto los sistemas locales como los recursos en la nube.

Se deben establecer procesos operativos que aseguren la continuidad del negocio, tales como planes de recuperación ante desastres, esquemas de escalabilidad de infraestructura y políticas de gobernanza adaptadas al entorno cloud.

La capacitación constante del personal técnico en herramientas cloud y metodologías de DevOps es indispensable para garantizar la efectividad operativa.

Además, el liderazgo organizacional debe promover una cultura de innovación y adaptación tecnológica que permita la adopción y el uso eficiente de las soluciones en la nube.

Dimensión del Entorno:

La dimensión ambiental incluye factores externos como la regulación gubernamental, las políticas de cumplimiento y las presiones competitivas que afectan la operación en la nube.

Las organizaciones deben garantizar que sus operaciones en la nube cumplan con normativas locales e internacionales relacionadas con la seguridad de los datos, la privacidad y la sostenibilidad ambiental.

Es clave adoptar soluciones cloud que permitan responder con agilidad a las demandas del mercado, como la capacidad de escalar servicios durante picos de uso o implementar nuevas tecnologías conforme evolucionan las necesidades del sector.

Colaborar con proveedores cloud confiables y participar en comunidades tecnológicas puede ofrecer acceso a mejores prácticas y recursos adicionales para mejorar la operación.

El TOE Framework, enfocado en la operación cloud, proporciona una estructura integral para alinear las capacidades tecnológicas, las prácticas organizacionales y las dinámicas externas, asegurando

un entorno híbrido eficiente, seguro y competitivo. Su aplicación en el contexto de Anónima SA resulta crucial para maximizar el valor de los servicios cloud mientras se mantiene la estabilidad operativa y se mitigan los riesgos asociados.

TAM (Technology Acceptance Model)

El TAM es un modelo clave para abordar la aceptación tecnológica por parte de los usuarios y su impacto en la operación cloud. Este modelo se centra en dos factores principales que determinan cómo los usuarios perciben e interactúan con las tecnologías implementadas en un entorno cloud híbrido:

Utilidad Percibida:

En el contexto de la operación cloud, la utilidad percibida se refiere al grado en que los usuarios consideran que las tecnologías en la nube mejoran su desempeño laboral. Es fundamental diseñar herramientas y plataformas cloud que faciliten tareas complejas, aumenten la eficiencia y reduzcan los tiempos de respuesta operativos.

Para fomentar esta percepción, se recomienda implementar dashboards personalizados que muestren el estado del sistema, automatizar procesos repetitivos y garantizar tiempos de actividad (uptime) elevados en los servicios cloud.

Facilidad de Uso Percibida:

Este factor evalúa la facilidad con la que los usuarios pueden interactuar con las plataformas y herramientas cloud. Diseñar interfaces intuitivas y accesibles que reduzcan la curva de aprendizaje es esencial para una adopción exitosa.

En un entorno cloud, esto implica proporcionar portales de autoservicio para la gestión de recursos, documentación clara y detallada, así como soporte técnico que garantice respuestas rápidas a consultas o problemas.

El TAM permite que las organizaciones enfoquen sus estrategias de adopción tecnológica en el diseño de soluciones funcionales y accesibles, promoviendo una operación cloud eficiente y reduciendo la resistencia al cambio.

Cloud Adoption Framework (CAF)

El Cloud Adoption Framework (CAF) es un marco integral diseñado para guiar a las organizaciones en la transición y operación de entornos cloud. Este enfoque estructurado permite no solo la adopción inicial de la nube, sino también su integración y optimización a largo plazo. Los componentes clave del CAF, enfocados en la operación cloud, incluyen:

Estrategia:

Se debe definir una estrategia clara que identifique los objetivos comerciales que se quieren alcanzar con la operación cloud. Esto incluye establecer indicadores clave de desempeño (KPIs) que midan la efectividad de la infraestructura cloud y su alineación con los objetivos del negocio.

Una estrategia efectiva también implica priorizar cargas de trabajo y servicios para migrarlos a la nube, basándose en su impacto en la continuidad del negocio y el retorno de inversión (ROI).

Planificación:

En la etapa de planificación, es fundamental mapear todas las dependencias de sistemas y aplicaciones críticas para garantizar una integración fluida en el entorno cloud.

Se deben asignar roles y responsabilidades dentro del equipo de TI para cubrir actividades específicas, como monitoreo de recursos, gestión de costos y cumplimiento normativo.

Además, la planificación debe incluir un calendario detallado que identifique hitos clave y recursos necesarios para ejecutar una operación cloud eficiente.

Governance:

La gobernanza en la operación cloud requiere establecer políticas claras que aseguren el cumplimiento normativo, la seguridad de los datos y el uso eficiente de los recursos.

Es esencial implementar herramientas de monitoreo y análisis que permitan visibilidad completa sobre las operaciones cloud. Esto incluye el uso de dashboards centralizados para identificar problemas, optimizar recursos y prever demandas futuras.

También se deben definir reglas de escalabilidad automática para gestionar de manera efectiva el uso de recursos durante picos de actividad o momentos de baja demanda.

Adopción y Operaciones:

La etapa de adopción implica garantizar que las aplicaciones y servicios sean desplegados de manera eficiente en la nube, con procedimientos que minimicen interrupciones en las operaciones.

La operación continua debe enfocarse en el monitoreo constante de la infraestructura, asegurando la alta disponibilidad y el rendimiento esperado.

También se deben implementar planes de recuperación ante desastres que automaticen la restauración de servicios en caso de fallos.

Optimización y Mejora Continua:

Finalmente, el CAF promueve un enfoque iterativo para optimizar los costos y el rendimiento en la nube. Esto incluye la revisión periódica de configuraciones, el ajuste dinámico de recursos y la evaluación de nuevas tecnologías que puedan integrarse al ecosistema existente.

El CAF proporciona una guía holística para garantizar que las operaciones en la nube sean seguras, escalables y alineadas con las necesidades empresariales. En el caso de Anónima SA, su implementación es esencial para maximizar la eficiencia operativa mientras se reducen riesgos y costos.

ITIL 4

ITIL 4 proporciona un marco adaptable y valioso para gestionar servicios de TI en un entorno cloud híbrido, garantizando que los procesos sean eficientes, escalables y centrados en el valor. Sus principios clave en la operación cloud híbrida incluyen:

Optimizar y Automatizar:

La automatización es fundamental en la operación cloud para reducir errores manuales, mejorar la eficiencia y garantizar la rapidez en la entrega de servicios. Por ejemplo, la implementación de scripts automatizados para despliegues, actualizaciones y recuperación ante fallos.

ITIL 4 impulsa también la optimización mediante herramientas de monitoreo en tiempo real que identifican cuellos de botella, permitiendo ajustes proactivos.

Entrega de Valor de Servicio:

En un entorno híbrido, ITIL 4 enfatiza la importancia de centrar los procesos operativos en la entrega continua de valor al cliente. Esto implica garantizar altos niveles de disponibilidad y proporcionar una experiencia de usuario uniforme en todos los entornos, ya sean on-premises o en la nube.

Colaborar y Promover la Visibilidad:

La colaboración entre equipos es esencial para gestionar un entorno cloud híbrido. ITIL 4 sugiere establecer reuniones de revisión operativa regulares y utilizar herramientas de gestión centralizada para compartir información clave.

Promover la visibilidad incluye reportar KPIs en dashboards accesibles, permitiendo una mejor toma de decisiones basada en datos.

Gestionar la Seguridad y el Riesgo:

ITIL 4 subraya la importancia de integrar la gestión de riesgos en la operación cloud híbrida, abordando temas como el acceso seguro, la protección de datos y la respuesta a incidentes.

Mejora Continua:

ITIL 4 recomienda mantener una cultura de mejora continua que se traduzca en optimizaciones regulares de los procesos cloud, como la reducción de costos operativos mediante el ajuste del uso de recursos o la adopción de nuevas tecnologías.

La aplicación de ITIL 4 en un entorno cloud híbrido permite a las organizaciones garantizar consistencia, escalabilidad y entrega de valor mientras minimizan riesgos y mejoran continuamente los servicios de TI.

Interoperabilidad y Gestión del Cambio

La interoperabilidad entre plataformas on-premises y cloud requiere:

Integración de Datos: Implementar herramientas como APIs y middleware que permitan el intercambio fluido de información.

Compatibilidad: Diseñar soluciones capaces de operar en entornos diversos sin interrupciones.

La gestión del cambio es fundamental para mitigar la resistencia organizacional mediante:

Capacitación: Diseñar programas de formación para garantizar que el personal esté preparado.

Estrategias de Comunicación: Establecer un plan claro para comunicar los beneficios y los cambios esperados.

Gestión del Cambio

La gestión del cambio es un componente esencial en la operación cloud, ya que permite garantizar una transición fluida hacia nuevos procesos y tecnologías mientras se mitiga la resistencia organizacional. Para asegurar una gestión del cambio efectiva en entornos cloud híbridos, se deben implementar las siguientes estrategias:

Capacitación del Personal:

Diseñar programas continuos de formación para que los empleados desarrollen las habilidades necesarias en herramientas y plataformas cloud.

Incluir sesiones específicas sobre seguridad, escalabilidad, y gestión de recursos en la nube para asegurar el dominio completo de las tecnologías implementadas.

Estrategias de Comunicación:

Implementar un plan de comunicación claro que explique los beneficios, objetivos y cambios esperados durante el proceso de transición a la nube.

Usar múltiples canales de comunicación, como reuniones, boletines y plataformas digitales, para mantener informados a los equipos en cada fase del proyecto.

Identificación y Empoderamiento de Agentes de Cambio:

Designar líderes internos que actúen como agentes de cambio, promoviendo la adopción de nuevas prácticas y sirviendo como punto de referencia para resolver inquietudes.

Capacitar a estos agentes para que puedan responder preguntas, motivar a sus compañeros y garantizar la alineación organizacional.

Medición del Impacto del Cambio:

Definir métricas claras para evaluar el progreso y la eficacia de las iniciativas de gestión del cambio, como la reducción en los tiempos de adaptación o el incremento en la productividad.

Usar encuestas y retroalimentación de los empleados para ajustar las estrategias según sea necesario.

Plan de Mitigación de Riesgos:

Identificar posibles riesgos asociados a la transición a la nube, como la resistencia al cambio o la curva de aprendizaje en nuevas herramientas.

Desarrollar planes de acción para abordar estos riesgos, asegurando una adaptación progresiva y efectiva.

Enfoque en la Experiencia del Usuario:

Priorizar la experiencia de los usuarios finales al implementar cambios en la operación cloud, garantizando que las nuevas tecnologías sean intuitivas y funcionales.

Recopilar datos de uso y retroalimentación para realizar mejoras continuas.

La gestión del cambio no solo facilita la adaptación de las organizaciones a entornos cloud híbridos, sino que también asegura que los equipos estén alineados con los objetivos estratégicos, promoviendo la eficiencia operativa y el éxito a largo plazo.

Seguridad y Cumplimiento

La seguridad y el cumplimiento son pilares fundamentales en la operación de un entorno cloud híbrido, ya que garantizan la protección de datos sensibles, el cumplimiento de normativas legales y la continuidad de las operaciones. La implementación de estrategias robustas y adaptadas al contexto cloud es esencial para mitigar riesgos y asegurar una operación confiable.

Políticas de Seguridad Proactivas:

Diseñar e implementar políticas de seguridad específicas para el entorno cloud, considerando la segmentación de redes, el control de acceso basado en roles y la gestión de identidades.

Establecer protocolos de seguridad avanzada, como el cifrado de datos en tránsito y en reposo, para proteger la información sensible contra accesos no autorizados.

Monitoreo y Detección en Tiempo Real:

Integrar herramientas de monitoreo continuo que detecten y alerten sobre actividades sospechosas o intentos de brechas de seguridad en la infraestructura cloud.

Implementar sistemas de respuesta automatizada a incidentes para minimizar el impacto de posibles amenazas.

Cumplimiento Normativo y Auditoría:

Garantizar el cumplimiento de normativas locales e internacionales, como GDPR, HIPAA o ISO 27001, según las necesidades específicas de la organización.

Realizar auditorías periódicas para evaluar el cumplimiento normativo y la eficacia de las políticas de seguridad.

Capacitación Continua en Seguridad:

Diseñar programas de capacitación para todos los empleados, con énfasis en las mejores prácticas de seguridad en la nube, como la gestión segura de contraseñas y la detección de intentos de phishing.

Realizar simulacros de respuesta ante incidentes para preparar a los equipos frente a posibles amenazas.

Estrategias de Recuperación y Continuidad:

Diseñar planes de recuperación ante desastres que incluyan copias de seguridad regulares, pruebas de restauración y estrategias de redundancia en la nube.

Asegurar la disponibilidad de los servicios críticos mediante arquitecturas de alta disponibilidad y escalabilidad automática.

Colaboración con Proveedores Cloud:

Establecer acuerdos claros con los proveedores cloud que incluyan responsabilidades compartidas en términos de seguridad y cumplimiento.

Evaluar regularmente las certificaciones y auditorías de seguridad de los proveedores para garantizar la confianza en su infraestructura.

La integración de estrategias de seguridad y cumplimiento en la operación cloud híbrida no solo protege los datos y sistemas, sino que también fomenta la confianza de los usuarios y clientes, permitiendo a las organizaciones operar en un entorno más seguro y alineado con las exigencias regulatorias.

Optimización de Recursos

La optimización de recursos es un aspecto esencial en la operación de entornos cloud, ya que permite maximizar el valor y minimizar los costos asociados al uso de la infraestructura. Implementar estrategias eficientes garantiza que los recursos sean utilizados de manera sostenible y alineada con las demandas del negocio. Los enfoques clave incluyen:

Monitoreo Activo de Recursos:

Implementar herramientas avanzadas de monitoreo en tiempo real que proporcionen visibilidad sobre el uso de CPU, memoria, almacenamiento y redes en el entorno cloud.

Configurar alertas automáticas para identificar recursos infrautilizados o sobrecargados, lo que permite ajustes inmediatos.

Escalabilidad Dinámica:

Diseñar arquitecturas que permitan escalar recursos automáticamente según las demandas del sistema. Esto incluye el uso de instancias elásticas y contenedores.

Ajustar la capacidad durante picos de uso y reducirla durante periodos de baja demanda para optimizar costos.

Uso de Modelos de Pago por Uso:

Adoptar estrategias de pago por uso ofrecidas por proveedores cloud para evitar costos fijos innecesarios.

Analizar los patrones de consumo y aprovechar descuentos por compromisos a largo plazo o instancias reservadas.

Optimización del Almacenamiento:

Clasificar y mover datos a niveles de almacenamiento menos costosos según su frecuencia de acceso y valor.

Implementar políticas de limpieza automática para eliminar datos obsoletos o duplicados, reduciendo costos de almacenamiento.

Automatización de Procesos Operativos:

Usar herramientas de orquestación y automatización para gestionar tareas recurrentes como implementaciones, copias de seguridad y actualizaciones.

Reducir la intervención manual en la gestión de recursos para mejorar la eficiencia.

Análisis de Costos y Rendimiento:

Realizar evaluaciones periódicas del costo-beneficio de los recursos utilizados en la nube.

Implementar dashboards que proporcionen información detallada sobre el gasto y el rendimiento, permitiendo tomar decisiones informadas.

Revisión y Ajuste Continuo:

Establecer un proceso de mejora continua para revisar y ajustar las configuraciones de los recursos.

Evaluar nuevas tecnologías y servicios ofrecidos por los proveedores cloud para garantizar una operación optimizada.

La optimización de recursos no solo asegura un uso eficiente de la infraestructura cloud, sino que también contribuye a la sostenibilidad financiera y operativa del modelo híbrido.

Metodología

Enfoque de la investigación

El estudio adopta un **enfoque cualitativo**, es el más adecuado, ya que el objetivo de la investigación es comprender cómo la organización puede adoptar un **modelo operativo híbrido en la gestión de entornos on-premises y cloud públicas**.

El enfoque cualitativo también permite una interpretación más rica de los datos, proporcionando **insights** que pueden ayudar en la formulación de mejores prácticas, recomendaciones estratégicas y una comprensión más profunda de los factores clave que afectan la integración de estos entornos tecnológicos.

Alcance de la investigación

El alcance de la investigación es exploratorio, lo que significa que busca comprender y analizar de manera preliminar los factores clave que influyen en la adopción de un modelo operativo híbrido en TI.

Este estudio exploratorio tiene como objetivo:

- Identificar y caracterizar las barreras y facilitadores de la transición a un modelo híbrido en la organización.
- Generar hipótesis y líneas de investigación futuras, al no existir estudios previos específicos sobre la gestión operativa en entornos híbridos dentro del contexto de Anónima SA.
- Explorar soluciones y estrategias a través del análisis de experiencias previas, modelos de referencia y mejores prácticas del sector.

El carácter exploratorio de la investigación implica que no se busca establecer relaciones causales o probar hipótesis predefinidas, sino descubrir elementos clave, estructurar conceptos y proponer enfoques innovadores para la integración de tecnologías híbridas.

Diseño de la investigación

El diseño del estudio es **no experimental y transversal**, ya que:

No experimental: No se manipulan variables, sino que se observan y analizan en su contexto natural. La información se obtiene a través de revisión documental, entrevistas con expertos y análisis cualitativo de datos.

Transversal: La recolección de información se realiza en un único momento del tiempo, permitiendo obtener una "fotografía" de la situación actual de Anónima SA en cuanto a su modelo operativo de TI.

Selección de métodos o instrumentos para recolección de información

Dado que el estudio es de tipo **descriptivo y basado en fuentes secundarias**, los métodos de recolección de información se enfocan en la selección y análisis de documentos relevantes.

Fuentes de información

Para garantizar la fiabilidad y validez de los datos recopilados, se utilizarán dos tipos principales de fuentes:

Base de datos Emis:

- Emis es una plataforma que proporciona informes de mercado, análisis sectoriales y estudios especializados sobre la industria tecnológica.
- Se consultarán documentos relacionados con la evolución de los modelos operativos en la gestión de TI, especialmente en empresas que han adoptado enfoques híbridos.

- Los reportes de tendencias en cloud computing y la integración de infraestructuras híbridas serán clave para contextualizar el estudio.

Documentos institucionales y normativos:

- Se revisarán informes generados por **organismos reguladores, entidades gubernamentales y gremios empresariales** que aborden la adopción de tecnologías en la nube.
- Se incluirán publicaciones de empresas tecnológicas líderes en el sector, tales como Amazon Web Services (AWS), Microsoft Azure y Google Cloud, que proporcionan directrices y recomendaciones sobre la gestión de entornos híbridos.
- También se analizarán estudios de caso de organizaciones que han implementado modelos operativos híbridos exitosamente.

Criterios de selección de documentos

Para garantizar la **calidad y relevancia** de la información, los documentos seleccionados deberán cumplir con los siguientes criterios:

- **Actualidad**: Preferiblemente publicaciones de los últimos cinco años.
- **Autoridad**: Provenientes de fuentes reconocidas como revistas científicas, informes de consultoras líderes (Gartner, Forrester, IDC) y normativas gubernamentales.
- **Relevancia**: Relacionados específicamente con la gestión de TI en entornos híbridos.
- **Accesibilidad**: Disponibles en bases de datos académicas, portales oficiales o con acceso institucional.

Técnicas de análisis de datos

Una vez seleccionados los documentos, se procederá a su análisis mediante **técnicas cualitativas**, que permitan extraer información relevante y formular conclusiones sólidas.

Principales técnicas de análisis utilizadas

Análisis de contenido

- Esta técnica permite identificar patrones, conceptos clave y tendencias en los textos revisados.
- Se examinan términos recurrentes y conceptos asociados con la adopción de modelos operativos de infraestructura híbrida, tales como gobierno, automatización, interoperabilidad, seguridad, eficiencia operativa y costos.
- Se aplicará un método de organización por categorías para clasificar la información en diferentes dimensiones temáticas.

Comparación temática

- Se compararán los enfoques propuestos por diferentes autores y organismos para la adopción de modelos cloud híbridos.
- Se examinarán similitudes y diferencias en cuanto a beneficios, riesgos y estrategias recomendadas.
- Esta técnica facilitará la identificación de **mejores prácticas aplicables a la gestión de TI en entornos híbridos**.

Síntesis de literatura

- Se elaborará un **marco conceptual consolidado** a partir de la revisión de los documentos seleccionados.

- Se integrarán teorías y modelos relevantes, como el **TOE Framework (Technology-Organization-Environment)** y el **Cloud Adoption Framework (CAF)**, para explicar la dinámica de la adopción tecnológica en empresas con infraestructura híbrida.
- Se generará un resumen analítico de los hallazgos más relevantes.

Análisis crítico y generación de recomendaciones

- A partir de la información analizada, se formularán **recomendaciones estratégicas** para la adopción de modelos operativos híbridos.
- Se evaluará el impacto de la implementación de estos modelos en términos de **costos, rendimiento, seguridad y gobernanza**.
- Se establecerán lineamientos que puedan ser utilizados por empresas interesadas en mejorar su gestión de TI mediante modelos híbridos.

Organización de la información

Para facilitar la estructuración del análisis, se presentará una **tabla resumen** que incluirá los siguientes elementos:

Tabla 1

Tabla de relación de revisión documental

Documento	Autor/Fuente	Técnica de análisis aplicada	Descripción de los hallazgos
Informe de Gartner sobre cloud híbrido	Gartner (2023)	Análisis de contenido	Identifica patrones y tendencias clave en la adopción de modelos de nubes híbridas en empresas de TI, enfocándose en gobernanza, seguridad, interoperabilidad y eficiencia operativa.
Estudio de caso sobre migración cloud en telecomunicaciones	IDC (2022)	Comparación temática	Evalúa diferencias en modelos de migración cloud en telecomunicaciones, analizando costos,

			riesgos y estrategias recomendadas.
The Processes of Technological Innovation	Tornatzky, L.G., & Fleischer, M. (1990)	Síntesis de literatura	Consolida modelos de innovación tecnológica aplicables a la adopción de infraestructura híbrida, integrando factores organizacionales y ambientales.
Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology	Davis, F.D. (1989)	Síntesis de literatura	Integra el modelo TAM para analizar la influencia de la percepción de utilidad y facilidad de uso en la adopción de servicios cloud.
The NIST Definition of Cloud Computing	Mell, P., & Grance, T. (2011)	Análisis de contenido	Define los principios fundamentales de la computación en la nube, categorizando los modelos de servicio e implementación.
ITIL Foundation, ITIL 4 Edition	AXELOS (2019)	Análisis crítico y generación de recomendaciones	Evalúa las mejores prácticas en la gestión de servicios de TI en entornos híbridos y proporciona recomendaciones estratégicas.
Azure Cloud Adoption Framework Handbook	Microsoft (2023)	Síntesis de literatura	Presenta un marco estructurado para la adopción de la nube, integrando modelos de madurez y estrategias de implementación.
Cloud Adoption Framework (CAF) de Microsoft	Microsoft (2023)	Síntesis de literatura	Explica la dinámica de adopción tecnológica en empresas con infraestructura híbrida, integrando modelos organizacionales y tecnológicos.

AWS Cloud Adoption Framework (AWS CAF)	Amazon Web Services (2023)	Comparación temática	Compara estrategias clave para la adopción de la nube, considerando gobernanza, seguridad y modelos operativos híbridos.
Google Cloud Adoption Framework	Google Cloud (2023)	Comparación temática	Evalúa la madurez organizacional en la adopción de la nube y compara estrategias de transformación digital.
A Proposed Framework for Cloud Computing Adoption	Victor Chang (2020)	Análisis de contenido	Identifica patrones y modelos organizacionales clave en la adopción de la computación en la nube.
Building a Framework to Drive Government Systems' Adoption of Cloud Computing	Nour Qatawneh (2024)	Análisis crítico y generación de recomendaciones	Examina el impacto de la adopción cloud en sistemas gubernamentales y formula recomendaciones basadas en gobernanza y sostenibilidad.

Análisis y discusión de los resultados

Este análisis de resultados se centra en la integración de infraestructuras de **nube pública** y **on-premise**, combinando los marcos conceptuales del **Cloud Adoption Framework (CAF)**, **ITIL** y el **Modelo de Aceptación Tecnológica (TAM)**. La interacción entre estas dos modalidades de infraestructura tecnológica representa un desafío significativo para las organizaciones que buscan modernizar sus operaciones, garantizar la interoperabilidad y optimizar recursos.

El **Cloud Adoption Framework (CAF)**, desarrollado por Microsoft, AWS y Google Cloud, se utiliza como base para estructurar y guiar el proceso de adopción de la nube pública. Este marco identifica elementos críticos como la gobernanza, seguridad y estrategias de migración, lo cual es esencial para garantizar una transición eficiente y sostenible desde sistemas tradicionales on-premise hacia entornos híbridos.

Complementariamente, **ITIL** proporciona un enfoque orientado a la gestión eficiente de servicios de TI. Sus buenas prácticas permiten alinear los objetivos estratégicos de las organizaciones con las capacidades operativas de infraestructuras híbridas, asegurando la continuidad del negocio y la calidad del servicio en contextos complejos que combinan nube pública y on-premise.

Por último, el **Modelo de Aceptación Tecnológica (TAM)** introduce una dimensión centrada en los usuarios finales y los tomadores de decisiones, evaluando cómo las percepciones de utilidad y facilidad de uso influyen en la aceptación de nuevas tecnologías. Esto resulta crucial para abordar las barreras organizacionales y culturales que pueden surgir al adoptar modelos híbridos de infraestructura tecnológica.

A través de esta integración de marcos teóricos, el análisis de resultados se explorará aspectos clave como la gobernanza, la interoperabilidad entre plataformas, la gestión del cambio organizacional y

la optimización de recursos. Al comprender las dinámicas que influyen en la adopción de infraestructuras híbridas, se busca proporcionar recomendaciones prácticas que impulsen la innovación y el rendimiento operativo en entornos que combinan nube pública e infraestructura on-premise.

Análisis de Limitaciones

El análisis ha identificado que el modelo actual de TI en Anónima SA, basado en la operación y gestión de infraestructura on-premises, depende de recursos locales y se estructura en silos organizacionales. Esto genera una serie de limitaciones:

Dependencia de recursos locales y silos organizacionales:

Descentralización de la infraestructura física: En un entorno de nube pública, la operación no requiere la gestión de servidores físicos ni redes locales, ya que esta responsabilidad recae en el proveedor. Los equipos tradicionales, sin embargo, están limitados por sus roles específicos, como administración de hardware, y carecen de habilidades necesarias para manejar APIs, herramientas de automatización o IaC (Infrastructure as Code) (Chang, 2020; Kovacevic & Dempsey, 2023).

Cambio hacia el consumo de servicios: En la nube, el enfoque cambia hacia la gestión de suscripciones, optimización de costos y configuración de servicios virtualizados. Los equipos, acostumbrados al mantenimiento físico, enfrentan retos significativos para adaptarse (NIST, 2011; Amazon Web Services, 2024).

Colaboración multidisciplinaria: Los entornos cloud demandan colaboración entre desarrollo, operaciones y seguridad (DevSecOps), rompiendo los silos tradicionales (Microsoft, 2023; Kovacevic & Dempsey, 2023).

Transformación de roles: La estructura de roles en la nube evoluciona hacia perfiles híbridos, como Cloud Engineers y Site Reliability Engineers (SREs), capaces de abarcar múltiples áreas tecnológicas (Alqatan et al., 2025).

Impactos prácticos:

Ineficiencias operativas y costos innecesarios debido a estructuras fragmentadas.

Desalineación organizacional que provoca duplicidades y problemas de gobernanza.

Falta de innovación y adopción de tecnologías avanzadas (Chang, 2020; Kovacevic & Dempsey, 2023).

Marcos de Trabajo

Cloud Adoption Framework (CAF)

El Cloud Adoption Framework (CAF) se ha convertido en un estándar clave para guiar a las organizaciones en su transición hacia la adopción de tecnologías en la nube. Diseñado inicialmente por Microsoft y adoptado con enfoques similares por proveedores como AWS y Google Cloud, el CAF proporciona un marco estructurado que abarca aspectos esenciales de la adopción cloud, tales como gobernanza, seguridad, optimización de costos y transformación organizacional (Microsoft, 2023; Amazon Web Services, 2024).

Los frameworks propuestos por los principales proveedores de nube se centran en prácticas comunes que abordan las necesidades críticas de las organizaciones. Estas prácticas incluyen la creación de landing zones para garantizar configuraciones iniciales seguras, el establecimiento de políticas de gobernanza automatizadas, la implementación de modelos de seguridad escalables y la promoción de la agilidad operativa. Asimismo, todos los frameworks enfatizan la importancia de la capacitación y el

cambio cultural, facilitando una adopción exitosa desde perspectivas tanto técnicas como organizacionales (Chang, 2020; Kovacevic & Dempsey, 2023).

Aunque cada framework tiene particularidades que reflejan las prioridades estratégicas de sus respectivos proveedores, las perspectivas del modelo CAF de AWS permiten un enfoque integral en los siguientes aspectos:

Perspectiva de Negocios

La **Perspectiva de Negocios** en los marcos de adopción de tecnologías en la nube, ya sea en nubes públicas, híbridas o entornos *on-premise*, se enfoca en garantizar que las decisiones tecnológicas estén alineadas con los objetivos comerciales y estratégicos de la organización. Este enfoque permite maximizar el retorno de inversión (ROI) y generar resultados medibles que impulsen la competitividad y sostenibilidad del negocio.

Elementos clave de la Perspectiva de Negocios

Alineación estratégica:

Las decisiones de adopción tecnológica deben estar directamente vinculadas con los objetivos comerciales. Esto incluye:

Mejorar la eficiencia operativa.

Reducir costos asociados a infraestructura o procesos.

Incrementar la agilidad organizacional para responder a cambios del mercado.

Acelerar la innovación en productos o servicios.

Es fundamental evaluar cómo la tecnología puede apoyar directamente en el logro de metas estratégicas específicas, como la expansión a nuevos mercados o el mejoramiento de la experiencia del cliente.

Análisis de casos de negocio:

Antes de implementar una solución tecnológica, se debe desarrollar un caso de negocio claro que identifique:

Los beneficios esperados (reducción de costos, aumento de ingresos, mejoras en la productividad).

Los costos asociados, tanto iniciales como recurrentes.

Los riesgos potenciales y su mitigación.

Además, es importante evaluar tanto el impacto inmediato como el valor a largo plazo para la organización.

Priorización basada en valor:

No todas las cargas de trabajo o aplicaciones tienen el mismo impacto en el negocio. Las iniciativas deben ser priorizadas en función de:

Su criticidad para las operaciones.

Su contribución directa a los ingresos o reducción de costos.

Su viabilidad técnica y nivel de complejidad.

Esta priorización asegura que los recursos (tanto humanos como financieros) se utilicen donde puedan generar el mayor impacto.

Medición de resultados:

Definir indicadores clave de rendimiento (KPIs) claros que permitan evaluar el impacto de la adopción tecnológica en términos comerciales, como:

Reducción del tiempo de lanzamiento de productos (*time-to-market*).

Incremento en la productividad de los equipos.

Mejoras en los niveles de satisfacción del cliente.

Monitorear y comunicar estos resultados periódicamente es esencial para garantizar el apoyo continuo de las partes interesadas.

Toma de decisiones basada en datos:

Implementar herramientas y procesos que permitan recopilar y analizar datos relevantes para la toma de decisiones estratégicas, como patrones de consumo, costos asociados y rendimiento de las aplicaciones.

Esto incluye tanto entornos de infraestructura local como soluciones en la nube, integrando datos de múltiples fuentes.

Beneficios de esta perspectiva en entornos híbridos

Optimización del gasto:

En un modelo híbrido, combinar infraestructuras *on-premise* con nubes públicas permite equilibrar costos según las necesidades del negocio, evitando el sobredimensionamiento de recursos.

Flexibilidad estratégica:

Adoptar soluciones híbridas o multi-nube permite a las organizaciones responder rápidamente a las demandas cambiantes del mercado, como escalar operaciones durante picos de demanda o reducir recursos durante períodos de menor actividad.

Mayor resiliencia:

La diversificación entre entornos *on-premise* y nubes públicas fortalece la continuidad del negocio, al garantizar redundancia y disponibilidad de servicios críticos.

Mejora de la experiencia del cliente:

Las tecnologías avanzadas, como análisis de datos en tiempo real o servicios personalizados, pueden implementarse más fácilmente con soluciones híbridas, asegurando que los clientes obtengan productos y servicios de alta calidad.

Buenas prácticas para implementar esta perspectiva

Definir una estrategia tecnológica clara:

Asegurarse de que la tecnología adoptada (ya sea en la nube o *on-premise*) esté alineada con los planes estratégicos a corto y largo plazo del negocio.

Involucrar a todas las partes interesadas:

Los líderes comerciales y tecnológicos deben trabajar juntos para garantizar que las prioridades del negocio estén representadas en las decisiones tecnológicas.

Adoptar un enfoque iterativo:

Realizar pruebas piloto antes de un despliegue completo, permitiendo a la organización validar los beneficios comerciales antes de comprometerse con una implementación a gran escala.

Capacitación continua:

Hay que asegurar que el personal, tanto técnico como no técnico, esté preparado para adoptar y aprovechar al máximo las nuevas herramientas y procesos.

Perspectiva de Personas

La **Perspectiva de Personas** se enfoca en cómo las organizaciones pueden preparar y capacitar a sus equipos para adoptar y gestionar eficientemente las tecnologías en la nube, modelos híbridos y entornos *on-premise*. Esta perspectiva reconoce que la transformación digital no se trata solo de tecnología, sino también de las personas que la implementan, gestionan y usan en su día a día.

El éxito de cualquier iniciativa tecnológica depende de que los equipos estén alineados con los objetivos estratégicos y tengan las habilidades y el compromiso necesarios para impulsar el cambio.

Componentes clave de la Perspectiva de Personas

Desarrollo de habilidades y capacitación continua:

- La adopción de nuevas tecnologías requiere que los equipos adquieran conocimientos técnicos y habilidades relacionadas con:

- Operación y gestión de entornos híbridos y multi-nube.
- Uso de herramientas específicas para automatización, monitoreo, y gestión de infraestructura.
- Prácticas modernas como DevOps, IaC (*Infrastructure as Code*), y enfoques ágiles.
- Las capacitaciones deben ser continuas para mantener al equipo actualizado frente a los rápidos avances tecnológicos.

Cambio cultural organizacional:

El cambio tecnológico debe ir acompañado de un cambio cultural que fomente:

La colaboración entre equipos de negocio, TI y operaciones.

La adopción de prácticas basadas en experimentación e innovación.

La aceptación del aprendizaje continuo y la mejora incremental.

Esto implica establecer una cultura que valore la agilidad, la resiliencia y la adaptabilidad.

Definición de roles y responsabilidades claras:

Es esencial que las organizaciones adapten sus estructuras para reflejar los cambios introducidos por la adopción de la nube y entornos híbridos, lo que incluye:

Roles específicos para la gestión de plataformas cloud y *on-premise*.

Responsabilidades claras para la seguridad, gobernanza y operación de los sistemas.

Creación de equipos interdisciplinarios que trabajen juntos para maximizar el valor del cambio tecnológico.

Gestión del cambio organizacional:

El proceso de adopción debe incluir un plan estructurado para gestionar el cambio, con etapas como:

Identificación de las áreas afectadas y los impactos en las personas.

Comunicación efectiva sobre los beneficios de la transformación.

Creación de incentivos para fomentar la participación y el compromiso de los equipos.

Atracción y retención de talento:

La transformación digital a menudo requiere atraer talento especializado en áreas como computación en la nube, big data, inteligencia artificial, y ciberseguridad.

Para retener talento, las organizaciones deben:

Crear planes de carrera claros.

Ofrecer oportunidades de crecimiento personal y profesional.

Establecer un entorno de trabajo flexible y dinámico.

Beneficios de la Perspectiva de Personas

Mayor productividad y eficiencia:

Los equipos bien capacitados pueden implementar y gestionar tecnologías más rápidamente, minimizando errores y aumentando la eficiencia operativa.

Adaptación a nuevas tecnologías:

Una fuerza laboral capacitada y con mentalidad abierta puede adoptar y utilizar rápidamente nuevas herramientas y plataformas, maximizando el valor de las inversiones tecnológicas.

Reducción de resistencia al cambio:

Al involucrar a las personas desde el inicio del proceso y comunicar claramente los beneficios, se disminuye la resistencia al cambio y se fomenta una adopción más fluida.

Innovación continua:

Equipos con acceso a capacitación y recursos son más propensos a innovar, experimentando con nuevas ideas y soluciones para resolver problemas empresariales.

Fortalecimiento de la resiliencia organizacional:

La combinación de habilidades técnicas y una cultura orientada al cambio prepara a las organizaciones para enfrentar desafíos y adaptarse rápidamente a entornos dinámicos.

Buenas prácticas para implementar la Perspectiva de Personas

Evaluar las brechas de habilidades:

Realizar evaluaciones regulares para identificar brechas en habilidades técnicas y blandas, y desarrollar planes de capacitación específicos para abordarlas.

Crear programas de capacitación personalizados:

Diseñar programas que se ajusten a las necesidades de los diferentes equipos, desde personal técnico hasta líderes de negocio.

Establecer un programa de comunicación continuo:

Comunicar constantemente los objetivos, beneficios y avances de la transformación tecnológica a todos los niveles de la organización.

Fomentar el liderazgo inclusivo:

Involucrar a líderes que sean agentes de cambio y modelos a seguir, promoviendo la adopción tecnológica y la colaboración.

Reconocer y recompensar el progreso:

Implementar incentivos para los equipos y colaboradores que adopten nuevas tecnologías y demuestren mejoras en su desempeño.

Casos prácticos de la Perspectiva de Personas

Capacitación en prácticas DevOps y Cloud:

Un equipo técnico puede ser capacitado en el uso de herramientas de automatización, como pipelines de CI/CD, para mejorar los tiempos de despliegue y la calidad del software.

Programas de mentoring interno:

Colaboradores con experiencia en entornos híbridos pueden actuar como mentores para otros, ayudando a acelerar la curva de aprendizaje.

Creación de un Centro de Excelencia (CoE):

Un CoE puede actuar como un grupo especializado para apoyar y guiar a los diferentes equipos en la adopción de tecnologías y mejores prácticas.

Perspectiva de Gobernanza

Estableciendo el control y la administración de la adopción tecnológica

La **Perspectiva de Gobernanza** en marcos de adopción tecnológica aborda los mecanismos, políticas y controles necesarios para garantizar que las organizaciones gestionen adecuadamente sus entornos tecnológicos, ya sea en la nube pública, híbrida o *on-premise*. Esta perspectiva asegura que las decisiones relacionadas con la tecnología estén alineadas con las políticas corporativas, regulaciones y metas estratégicas, reduciendo riesgos y optimizando recursos.

Componentes clave de la Perspectiva de Gobernanza

Definición de políticas claras:

Las organizaciones deben establecer políticas de gobernanza que definan cómo se gestionarán los recursos tecnológicos. Estas políticas incluyen:

Uso responsable de los recursos (por ejemplo, asignación de costos a áreas específicas o proyectos).

Definición de reglas para el acceso y uso de datos.

Directrices para el manejo de riesgos y cumplimiento normativo.

Control de acceso y gestión de identidades:

La gobernanza debe garantizar que solo las personas autorizadas tengan acceso a los sistemas, datos y recursos. Esto incluye:

Implementación de roles y permisos específicos para minimizar riesgos de acceso no autorizado.

Uso de principios como "mínimo privilegio necesario" y *Zero Trust* para reforzar la seguridad.

Auditorías regulares de usuarios y permisos.

Cumplimiento normativo y regulatorio:

La adopción de tecnología debe cumplir con las regulaciones locales e internacionales aplicables, como:

Regulaciones de privacidad (GDPR, HIPAA, etc.).

Normativas financieras o del sector específico.

Políticas internas de la organización.

Esto implica establecer procesos para realizar auditorías y reportes periódicos.

Automatización de la gobernanza:

Para asegurar consistencia y escalabilidad, se deben implementar herramientas que automaticen aspectos clave de la gobernanza, como:

Aplicación de políticas mediante *Infrastructure as Code*.

Automatización de etiquetado de recursos para la gestión de costos y uso eficiente.

Monitoreo en tiempo real para identificar y mitigar desviaciones.

Gestión del ciclo de vida de los recursos:

La gobernanza debe cubrir todo el ciclo de vida de los recursos tecnológicos, desde la adquisición hasta la desactivación, incluyendo:

Establecimiento de procesos para la creación y eliminación de recursos.

Evaluación continua de los recursos para garantizar que sean necesarios y eficientes.

Identificación de recursos ociosos o sobre aprovisionados.

Métricas e informes de gobernanza:

Definir métricas clave para evaluar la efectividad de la gobernanza, como:

Porcentaje de cumplimiento de políticas de seguridad.

Costos asociados a recursos no etiquetados o ineficientes.

Frecuencia de auditorías y reportes regulatorios exitosos.

Implementar herramientas que generen reportes regulares para los responsables de la toma de decisiones.

Beneficios de la Perspectiva de Gobernanza

Control de costos y optimización de recursos:

Establecer políticas claras y automatizadas reduce el gasto innecesario en recursos tecnológicos y asegura su uso eficiente.

Mitigación de riesgos:

La gobernanza ayuda a identificar y gestionar riesgos relacionados con seguridad, cumplimiento y uso indebido de los recursos.

Cumplimiento normativo garantizado:

Con procesos y herramientas adecuados, las organizaciones pueden cumplir con regulaciones internas y externas sin comprometer su eficiencia.

Escalabilidad organizada:

A medida que las organizaciones crecen o adoptan nuevos entornos tecnológicos, la gobernanza asegura que esta expansión se realice de manera controlada y sostenible.

Transparencia y rendición de cuentas:

Los informes y métricas regulares permiten a los líderes comprender el estado de los recursos tecnológicos y tomar decisiones informadas.

Buenas prácticas para implementar la Perspectiva de Gobernanza

Crear un marco de gobernanza adaptable:

Diseñar políticas que puedan ajustarse a los cambios tecnológicos, regulatorios y organizacionales.

Implementar herramientas de monitoreo y auditoría:

Usar plataformas que permitan rastrear el uso de recursos, evaluar el cumplimiento normativo y detectar irregularidades en tiempo real.

Involucrar a las partes interesadas:

Hay que asegurar que todas las áreas relevantes (TI, legal, finanzas, operaciones) participen en la definición y aplicación de políticas de gobernanza.

Fomentar la transparencia:

Establecer procesos que permitan a todos los niveles organizacionales comprender y cumplir las políticas de gobernanza.

Capacitar a los equipos:

Ofrecer formación continua para que los colaboradores entiendan su papel en la gobernanza y sepan cómo aplicar las políticas en sus tareas diarias.

Casos prácticos de la Perspectiva de Gobernanza

Etiquetado automatizado de recursos:

Implementar un sistema que asigne etiquetas automáticamente a los recursos tecnológicos, clasificándolos por proyecto, departamento o propietario. Esto facilita la administración de costos y el cumplimiento de políticas internas.

Cumplimiento de seguridad automatizado:

Usar herramientas que evalúen continuamente los entornos tecnológicos en busca de configuraciones no seguras o que no cumplan con las políticas definidas, y que apliquen correcciones automáticas.

Gestión centralizada de identidades y accesos:

Implementar una solución centralizada para gestionar identidades que permita controlar quién tiene acceso a qué recursos, y realizar auditorías regulares.

Procesos de aprobación para recursos críticos:

Establecer flujos de trabajo donde los recursos críticos, como servidores de producción, solo puedan ser creados o modificados previa aprobación de los responsables

Perspectiva de Plataforma

Se centra en diseñar, implementar y mantener una arquitectura tecnológica sólida y escalable que permita soportar las operaciones, aplicaciones y servicios de la organización. En el contexto de nubes públicas, entornos híbridos y *on-premise*, esta perspectiva asegura que la infraestructura tecnológica esté optimizada para cumplir con los requisitos operativos, de rendimiento y de seguridad, mientras se mantiene alineada con los objetivos del negocio.

Componentes clave de la Perspectiva de Plataforma:

Diseño e implementación de Landing Zones:

Las *Landing Zones* son entornos base preconfigurados que sirven como punto de partida para implementar recursos tecnológicos. Incluyen configuraciones estándar para:

Redes seguras y segmentadas.

Control de acceso y gestión de identidades.

Políticas de gobernanza, como etiquetado de recursos y límites de costos.

Configuración inicial de herramientas de monitoreo y seguridad.

En entornos híbridos, las *Landing Zones* pueden extenderse para incluir integraciones entre la infraestructura *on-premise* y los entornos en la nube.

Estandarización y automatización de la infraestructura:

Implementar *Infrastructure as Code* (IaC) para crear y gestionar recursos de manera automática y replicable, garantizando que todas las configuraciones sigan los mismos estándares.

Herramientas de IaC permiten:

Reducción de errores manuales.

Despliegues consistentes en múltiples entornos (desarrollo, pruebas, producción).

Escalabilidad rápida en respuesta a las demandas del negocio.

Diseño para escalabilidad y resiliencia:

La plataforma debe diseñarse para soportar picos de demanda y garantizar alta disponibilidad. Esto incluye:

Uso de arquitecturas distribuidas y balanceo de carga.

Implementación de servicios que puedan escalar horizontalmente para manejar el crecimiento de usuarios o datos.

Respaldo mediante estrategias de recuperación ante desastres (*disaster recovery*).

Integración híbrida y conectividad:

En un modelo híbrido, la plataforma debe permitir la integración fluida entre la infraestructura local (*on-premise*) y los servicios en la nube. Esto incluye:

Configuración de redes privadas virtuales (VPN) o conexiones dedicadas de alta velocidad.

Sincronización de datos entre entornos para asegurar consistencia y disponibilidad.

Compatibilidad con múltiples proveedores de nube para evitar bloqueos tecnológicos (*vendor lock-in*).

Monitoreo y Observabilidad:

Implementar soluciones de monitoreo que proporcionen visibilidad en tiempo real sobre el rendimiento, la disponibilidad y la seguridad de la plataforma. Esto incluye:

Monitoreo de infraestructura (CPU, memoria, red).

Monitoreo de aplicaciones y servicios (rendimiento, tiempos de respuesta).

Generación de alertas para identificar y resolver problemas proactivamente.

Optimización del rendimiento y costos:

La plataforma debe configurarse para maximizar el rendimiento al menor costo posible. Esto incluye:

Uso de instancias o recursos bajo demanda, reservados o spot, según las necesidades.

Identificación y eliminación de recursos ociosos.

Ajuste automático de recursos para responder a cambios en la carga de trabajo.

Beneficios de la Perspectiva de Plataforma

Base tecnológica escalable y confiable:

Diseñar una plataforma robusta permite a las organizaciones responder rápidamente a las demandas del negocio y garantizar la continuidad operativa.

Eficiencia operativa:

La estandarización y automatización de la infraestructura reduce el tiempo necesario para implementar y gestionar recursos, liberando al equipo para enfocarse en tareas estratégicas.

Agilidad en la innovación:

Una plataforma bien diseñada permite a los equipos experimentar, implementar y mejorar productos o servicios con mayor rapidez.

Reducción de costos:

Al optimizar el uso de recursos y minimizar el desperdicio, las organizaciones pueden reducir significativamente los costos operativos asociados con la infraestructura tecnológica.

Integración fluida entre entornos:

Las plataformas híbridas bien integradas permiten aprovechar lo mejor de la nube pública y las infraestructuras *on-premise*, mejorando la flexibilidad y la interoperabilidad.

Buenas prácticas para implementar la Perspectiva de Plataforma

Adoptar un enfoque modular:

Diseñar la plataforma como un conjunto de componentes modulares e independientes que puedan integrarse y escalarse según sea necesario.

Estandarizar configuraciones iniciales:

Definir plantillas y configuraciones base para todos los entornos tecnológicos, asegurando consistencia y cumplimiento de políticas.

Automatizar tanto como sea posible:

Usar herramientas de IaC y automatización para minimizar errores manuales y facilitar la repetición de procesos en múltiples entornos.

Implementar pruebas continuas:

Establecer mecanismos de pruebas automatizadas para garantizar que los cambios en la plataforma no afecten su estabilidad ni seguridad.

Monitorear y ajustar regularmente:

Revisar periódicamente el rendimiento y el uso de la plataforma para identificar oportunidades de mejora y optimización.

Casos prácticos de la Perspectiva de Plataforma

Migración a un entorno híbrido:

Una organización que opera en *on-premise* implementa una conexión segura entre su datacenter local y un proveedor de nube pública para extender sus capacidades y manejar picos de demanda.

Automatización de despliegues de aplicaciones:

Usar IaC para configurar automáticamente servidores, bases de datos y redes en múltiples entornos, garantizando consistencia y ahorrando tiempo.

Optimización de costos en la nube:

Identificar y eliminar recursos no utilizados, como máquinas virtuales o discos sin uso, reduciendo significativamente el gasto mensual.

Recuperación ante desastres:

Configurar copias de seguridad automáticas y planes de recuperación en diferentes regiones o entornos para garantizar la continuidad del negocio ante fallos.

Perspectiva de Seguridad

Es fundamental para garantizar la protección de los datos, aplicaciones e infraestructura en entornos tecnológicos que incluyen nubes públicas, híbridas y *on-premise*. Este enfoque abarca estrategias, herramientas y procesos diseñados para mitigar riesgos, prevenir vulnerabilidades y cumplir con requisitos normativos, sin comprometer la agilidad y eficiencia operativa de las organizaciones.

Componentes clave de la Perspectiva de Seguridad:

Modelo de responsabilidad compartida:

En entornos de nube pública, híbrida y *on-premise*, la seguridad es una responsabilidad compartida entre los proveedores de servicios y la organización.

Proveedor: Asegura la infraestructura física, redes y servicios base.

Organización: Es responsable de proteger las aplicaciones, datos, accesos y configuraciones dentro del entorno.

Comprender y definir claramente esta responsabilidad es esencial para una implementación segura.

Gestión de identidades y accesos (IAM):

Controlar el acceso a recursos y datos es crítico. Esto incluye:

Uso del principio de privilegios mínimos, asegurando que los usuarios solo tengan acceso a los recursos necesarios.

Autenticación multifactor (MFA) para todas las cuentas críticas.

Implementación de roles, grupos y políticas bien definidas para gestionar accesos de manera escalable.

Auditorías regulares de cuentas y accesos.

Protección de datos:

La protección de los datos en reposo y en tránsito es clave. Esto incluye:

Uso de cifrado robusto para datos sensibles tanto en almacenamiento como durante la transferencia.

Implementación de políticas de retención y eliminación seguras para garantizar que los datos solo se almacenen mientras sea necesario.

Clasificación de datos para identificar y priorizar la protección de información crítica.

Gestión de vulnerabilidades:

Identificar y mitigar vulnerabilidades en aplicaciones e infraestructura. Esto incluye:

Análisis regulares de vulnerabilidades con herramientas de escaneo automatizado.

Aplicación rápida de parches y actualizaciones de seguridad.

Pruebas de penetración periódicas para simular ataques y evaluar la robustez de los sistemas.

Monitoreo y detección de amenazas:

Establecer sistemas de monitoreo en tiempo real para detectar y responder a amenazas antes de que se conviertan en incidentes mayores. Esto incluye:

Implementación de herramientas de monitoreo continuo y alertas para identificar actividades sospechosas.

Uso de sistemas de detección y respuesta ante amenazas (EDR, XDR, SIEM).

Establecimiento de un equipo o proceso de respuesta ante incidentes (CSIRT).

Cumplimiento normativo:

Asegurar el cumplimiento de normativas locales e internacionales, tales como:

GDPR (Reglamento General de Protección de Datos).

ISO 27001 (gestión de seguridad de la información).

Normativas específicas de sectores como PCI DSS (industria de pagos) o HIPAA (sector salud).

Esto implica realizar auditorías periódicas y mantener documentación actualizada sobre los procesos de seguridad.

Estrategias de respuesta ante incidentes:

Diseñar y probar un plan de respuesta ante incidentes que permita a la organización reaccionar rápidamente frente a ataques o fallos. Esto incluye:

Simulacros regulares de respuesta para preparar a los equipos.

Creación de un plan de continuidad del negocio y recuperación ante desastres.

Documentación clara de roles y responsabilidades en caso de incidentes.

Cultura de ciberseguridad:

Fomentar una cultura organizacional orientada a la seguridad mediante:

Capacitación continua para los empleados, enfocada en identificar y prevenir ataques como el phishing.

Concienciación sobre las mejores prácticas de seguridad en el uso diario de herramientas tecnológicas.

Incentivar a los equipos a reportar actividades sospechosas.

Beneficios de la Perspectiva de Seguridad

Protección contra ciberamenazas:

Una estrategia sólida de seguridad reduce el riesgo de ataques como ransomware, phishing o accesos no autorizados.

Cumplimiento normativo y reputacional:

Garantizar la conformidad con regulaciones no solo evita sanciones legales, sino que también protege la reputación de la organización frente a clientes y socios.

Continuidad del negocio:

La implementación de estrategias de recuperación ante desastres y respuesta a incidentes asegura que los servicios puedan mantenerse operativos incluso frente a eventos críticos.

Confianza de clientes y socios:

Al demostrar un compromiso con la seguridad, las organizaciones generan confianza en sus clientes, socios y partes interesadas.

Reducción de costos a largo plazo:

Prevenir brechas de seguridad y ataques cibernéticos evita costos significativos asociados a la recuperación y pérdida de datos.

Buenas prácticas para implementar la Perspectiva de Seguridad

Integrar la seguridad desde el diseño:

Incorporar principios de seguridad desde el inicio del diseño de aplicaciones, servicios e infraestructura (*Security by Design*).

Adoptar una mentalidad de Zero Trust:

No asumir confianza en ningún usuario, dispositivo o red, verificando constantemente la identidad y los permisos antes de otorgar acceso.

Automatizar procesos de seguridad:

Usar herramientas que permitan monitorear, detectar y responder automáticamente a amenazas, optimizando el tiempo y recursos del equipo.

Auditorías y evaluaciones regulares:

Realizar revisiones periódicas de configuraciones, accesos y políticas de seguridad para identificar y corregir debilidades.

Fomentar la colaboración interdepartamental:

Involucrar a todas las áreas de la organización en la estrategia de seguridad, asegurando que todos los equipos entiendan y cumplan con los estándares definidos.

Casos prácticos de la Perspectiva de Seguridad

Cifrado de datos sensibles:

Una empresa financiera implementa cifrado de extremo a extremo para proteger los datos de sus clientes en reposo y durante la transferencia.

Análisis proactivo de amenazas:

Una organización utiliza herramientas de análisis de vulnerabilidades para identificar riesgos en sus aplicaciones antes de que se conviertan en puntos de ataque.

Planes de respuesta ante ransomware:

Una empresa de manufactura establece un plan de contingencia para restaurar sus operaciones rápidamente en caso de un ataque de ransomware.

Capacitación contra phishing:

Un minorista capacita a sus empleados para reconocer correos electrónicos sospechosos y prevenir el acceso a sistemas internos por parte de atacantes.

Perspectiva de Operaciones

Se centra en los procesos, herramientas y prácticas necesarias para gestionar y optimizar las operaciones tecnológicas en entornos de nubes públicas, híbridas y *on-premise*. Su objetivo principal es garantizar la continuidad del negocio, la eficiencia operativa y la capacidad de adaptación a cambios o incidentes inesperados, al tiempo que se mantienen altos niveles de disponibilidad y rendimiento.

Componentes clave de la Perspectiva de Operaciones

Monitoreo proactivo y observabilidad:

Implementar herramientas y procesos que proporcionen visibilidad en tiempo real sobre la infraestructura y las aplicaciones. Esto incluye:

Monitoreo de recursos tecnológicos (CPU, memoria, almacenamiento, red).

Seguimiento del rendimiento de aplicaciones y servicios críticos.

Observabilidad avanzada que permita rastrear transacciones y métricas específicas de negocio.

Alertas configuradas para notificar eventos como sobrecarga de recursos, interrupciones o patrones anómalos.

Gestión del ciclo de vida de los recursos:

Garantizar que los recursos tecnológicos sean gestionados de manera eficiente desde su creación hasta su desactivación. Esto implica:

Automatización de la provisión y des aprovisionamiento de recursos para evitar desperdicios.

Evaluación continua de la capacidad para ajustarla a la demanda.

Uso de políticas de optimización para mantener recursos actualizados y alineados con las necesidades operativas.

Automatización de operaciones:

Reducir el trabajo manual mediante herramientas que permitan automatizar procesos repetitivos. Ejemplos incluyen:

Implementación de *Infrastructure as Code* (IaC) para gestionar entornos híbridos de manera consistente.

Automatización de tareas de mantenimiento, como actualizaciones de software, parches de seguridad y creación de copias de seguridad.

Uso de flujos de trabajo automatizados para gestionar incidentes y solicitudes.

Gestión de incidentes y problemas:

Establecer procesos claros para responder y resolver incidentes de manera rápida y efectiva. Esto incluye:

Uso de sistemas de registro centralizado de incidentes para rastrear y priorizar problemas.

Identificación de la causa raíz de los problemas para evitar recurrencias.

Implementación de planes de comunicación para informar a las partes interesadas durante interrupciones.

Escalabilidad y continuidad del negocio:

Diseñar sistemas que puedan escalar según las necesidades operativas y garantizar la disponibilidad continua de los servicios. Esto implica:

Configuración de mecanismos de escalado horizontal y vertical.

Implementación de estrategias de recuperación ante desastres (DR) con respaldos geográficamente distribuidos.

Realización de simulacros para validar la capacidad de recuperación y respuesta de los sistemas.

Optimización de costos operativos:

Supervisar el uso de los recursos para identificar oportunidades de ahorro. Esto incluye:

Ajuste de recursos ociosos o subutilizados.

Uso de análisis predictivo para optimizar el gasto en entornos de nube según patrones de uso.

Evaluaciones regulares de costos frente al rendimiento.

Gestión del conocimiento operativo:

Crear y mantener documentación clara y actualizada sobre las operaciones tecnológicas. Esto incluye:

Manuales de procedimientos operativos.

Base de conocimientos sobre resolución de problemas comunes.

Registro de cambios y configuraciones para garantizar trazabilidad.

Beneficios de la Perspectiva de Operaciones

Mejora de la eficiencia operativa:

La automatización y estandarización reducen la carga operativa, permitiendo a los equipos enfocarse en actividades estratégicas.

Mayor disponibilidad de servicios:

Al monitorear y gestionar proactivamente los recursos, las organizaciones pueden garantizar niveles altos de disponibilidad y minimizar interrupciones.

Reducción del tiempo de respuesta:

Procesos bien definidos y herramientas de monitoreo permiten identificar y resolver incidentes de manera más rápida.

Optimización de costos:

Al alinear los recursos con la demanda y automatizar la gestión, las organizaciones pueden operar de manera más rentable.

Continuidad del negocio garantizada:

Estrategias de escalabilidad y recuperación ante desastres aseguran que los servicios permanezcan operativos incluso frente a eventos críticos.

Buenas prácticas para implementar la Perspectiva de Operaciones

Adoptar un enfoque de operaciones basado en datos:

Recopilar y analizar métricas clave para identificar áreas de mejora y tomar decisiones informadas.

Implementar operaciones resilientes:

Diseñar sistemas con redundancia y tolerancia a fallos para garantizar la continuidad del servicio.

Automatizar la mayor cantidad posible de tareas:

Usar herramientas de orquestación y scripts para automatizar actividades repetitivas y reducir errores humanos.

Realizar simulacros regulares:

Probar planes de recuperación y respuesta para garantizar que estén actualizados y que los equipos estén preparados para manejar incidentes.

Fomentar una cultura de mejora continua:

Involucrar a los equipos operativos en revisiones periódicas de procesos y resultados, incentivando la innovación y la optimización.

Casos prácticos de la Perspectiva de Operaciones

Monitoreo proactivo de aplicaciones críticas:

Una organización utiliza herramientas de observabilidad para rastrear el rendimiento de sus aplicaciones clave, identificando problemas antes de que afecten a los usuarios finales.

Automatización de copias de seguridad:

Un banco implementa flujos automatizados para realizar respaldos regulares de sus datos críticos, garantizando su disponibilidad en caso de fallos.

Gestión optimizada de costos en la nube:

Una empresa tecnológica realiza análisis periódicos de uso en su entorno híbrido, ajustando automáticamente recursos subutilizados para ahorrar costos.

Planes de recuperación ante desastres probados:

Una compañía de retail realiza simulacros trimestrales de recuperación ante desastres, asegurando que pueda reanudar operaciones en menos de 30 minutos tras un fallo.

ITIL en un Entorno Híbrido (Nube Pública y On-Premise)

ITIL (Information Technology Infrastructure Library) es un marco de referencia líder en la gestión de servicios de TI (ITSM), diseñado para alinear las operaciones tecnológicas con las necesidades del negocio. En un entorno híbrido que combina infraestructura on-premise y nube pública, ITIL proporciona prácticas probadas para garantizar la eficiencia operativa, la continuidad del servicio y el cumplimiento de los objetivos estratégicos.

Plan de Desarrollo ITIL para Entornos Híbridos

1. Estrategia del Servicio

   La estrategia del servicio en ITIL se enfoca en definir cómo los servicios de TI aportan valor al negocio.

Definición del portafolio de servicios híbridos:

Clasificar servicios según su ubicación (on-premise o nube pública) y su impacto estratégico.

Priorizar servicios críticos que aprovechen la elasticidad de la nube, como aplicaciones web o analítica avanzada.

Gestión financiera del servicio:

Implementar modelos de costos basados en el consumo para la nube pública.

Establecer métricas para medir el ROI de la migración y operación híbrida.

Gestión de la demanda:

Desarrollar capacidades para anticipar la demanda, utilizando herramientas analíticas en tiempo real.

2. Diseño del Servicio

El diseño del servicio asegura que los servicios nuevos y los existentes sean efectivos y cumplan con las expectativas del cliente.

Diseño de servicios híbridos:

Crear arquitecturas que integren de manera fluida componentes on-premise y en la nube.

Garantizar la interoperabilidad mediante estándares abiertos y APIs.

Gestión del catálogo de servicios:

Crear un catálogo centralizado que incluya detalles de los servicios híbridos, como SLA, costos y ubicaciones.

Gestión de seguridad de la información:

Implementar políticas de seguridad basadas en estándares como ISO 27001 para proteger datos en tránsito y en reposo.

Aplicar el modelo de responsabilidad compartida en la nube, definiendo claramente las responsabilidades del proveedor cloud y de los equipos internos.

3. Transición del Servicio

La transición del servicio asegura que las nuevas implementaciones o cambios en los servicios existentes se realicen de manera controlada.

Gestión de cambios:

Adoptar un enfoque ágil para gestionar cambios en entornos híbridos, minimizando el impacto en el servicio.

Establecer canales de aprobación para cambios críticos que afecten la conectividad o la seguridad.

Gestión de la configuración:

Crear una base de datos de gestión de la configuración (CMDB) que integre recursos locales y en la nube.

Pruebas y validación del servicio:

Realizar pruebas en entornos híbridos simulando escenarios reales para validar la funcionalidad, la seguridad y el rendimiento.

4. Operación del Servicio

La operación del servicio garantiza la entrega diaria de los servicios de TI de manera confiable y eficiente.

Gestión de eventos:

Implementar herramientas de monitoreo como AWS CloudWatch, Azure Monitor o Zabbix para detectar y responder a eventos en tiempo real.

Priorizar la automatización de la respuesta a incidentes comunes.

Gestión de incidentes:

Definir un flujo de trabajo integrado para manejar incidentes en entornos híbridos, con una visión unificada del estado de los servicios.

Gestión de problemas:

Establecer un proceso de análisis de causa raíz para incidentes recurrentes, priorizando la resolución de problemas que afectan tanto a la nube como a la infraestructura local.

5. Mejora Continua del Servicio

La mejora continua se centra en optimizar los servicios de TI y los procesos para maximizar su valor.

Evaluación de desempeño:

Implementar KPIs para medir la eficiencia de los servicios híbridos, como disponibilidad, tiempo de recuperación y costos.

Revisión de procesos:

Realizar auditorías periódicas de los procesos de ITIL para identificar áreas de mejora.

Ciclo de retroalimentación:

Recolectar datos de los usuarios finales y stakeholders para ajustar continuamente los servicios a sus necesidades.

Estrategias de Implementación de ITIL

Capacitación del Personal

Diseñar programas de formación en ITIL específicos para equipos que gestionen servicios híbridos.

Promover certificaciones ITIL entre los líderes y operadores clave.

Integración de Herramientas

Implementar plataformas como ServiceNow o BMC Helix para gestionar incidentes, cambios y problemas en un solo sistema.

Automatizar flujos de trabajo críticos utilizando soluciones de gestión de servicios ITSM.

Enfoque en la Automatización

Utilizar IaC para implementar y gestionar recursos, asegurando consistencia y control en entornos híbridos.

Automatizar tareas repetitivas, como la escalabilidad de servicios o la aplicación de parches de seguridad.

Gobernanza y Cumplimiento

Establecer un comité de gobernanza que supervise la implementación de ITIL y asegure el cumplimiento de normativas.

Definir políticas de seguridad y privacidad que cubran tanto la nube como la infraestructura on-premise.

Beneficios Esperados

Mayor Eficiencia Operativa:

Optimización de procesos y servicios a través de prácticas estructuradas y estándares probados.

Mayor Disponibilidad y Resiliencia:

Reducción de tiempos de inactividad gracias a prácticas de gestión de incidentes y eventos integradas.

Cumplimiento Normativo:

Garantía de que las operaciones híbridas cumplen con las normativas locales e internacionales.

Alineación Estratégica:

Asegurar que los servicios híbridos aporten valor directo al negocio y respalden sus objetivos.

Mejora Continua:

Capacidad de evolucionar los servicios para adaptarse a cambios en las necesidades del negocio o avances tecnológicos.

Modelo de Aceptación Tecnológica (TAM) en un Entorno Híbrido

El **Modelo de Aceptación Tecnológica (TAM)**, desarrollado por Fred Davis, es una herramienta clave para comprender cómo las percepciones de los usuarios influyen en la adopción y uso de nuevas tecnologías. En el contexto de un entorno híbrido que combina nube pública e infraestructura on-premise, TAM puede ayudar a garantizar que la transición tecnológica sea aceptada por los equipos internos, al identificar y abordar las barreras relacionadas con la percepción de utilidad y facilidad de uso.

Componentes Clave del TAM Aplicados al Entorno Híbrido

1. Percepción de Utilidad (PU)

Definición: Grado en que los usuarios perciben que la tecnología mejorará su desempeño laboral.

Aplicación al entorno híbrido:

Comunicar cómo los servicios híbridos pueden mejorar la productividad, como escalabilidad, automatización de tareas y tiempos de respuesta más rápidos.

Presentar casos prácticos que demuestren beneficios tangibles, como la reducción del tiempo de procesamiento de datos o la mejora en la experiencia del cliente.

2. Percepción de Facilidad de Uso (PEOU)

Definición: Grado en que los usuarios perciben que la tecnología es fácil de entender y utilizar.

Aplicación al entorno híbrido:

Simplificar los procesos de adopción tecnológica mediante herramientas intuitivas y interfaces de usuario amigables.

Proveer tutoriales, guías y formación para garantizar que los usuarios se sientan cómodos utilizando las nuevas plataformas.

3. Actitud hacia el Uso (ATU)

Definición: Sentimientos positivos o negativos hacia el uso de la tecnología.

Aplicación al entorno híbrido:

Fomentar actitudes positivas resaltando los beneficios individuales y organizacionales de la tecnología híbrida.

Identificar y abordar resistencias al cambio, como temores relacionados con la complejidad o la pérdida de control.

4. Intención de Uso (BI)

Definición: La intención de los usuarios de adoptar la tecnología.

Aplicación al entorno híbrido:

Crear campañas de concienciación interna que expliquen los objetivos estratégicos y operativos de la adopción híbrida.

Utilizar métricas de aceptación para medir la disposición de los usuarios hacia las nuevas tecnologías.

Plan de Desarrollo del TAM en un Entorno Híbrido

1. Análisis Inicial

Encuestas de percepción: Recopilar datos sobre cómo los usuarios perciben la utilidad y la facilidad de uso de las herramientas híbridas.

Identificación de resistencias: Mapear los posibles puntos de fricción, como la falta de conocimiento técnico o preocupaciones sobre la seguridad.

2. Diseño de la Estrategia de Adopción

Demostración de beneficios:

Presentar casos de éxito internos o externos para ilustrar cómo la tecnología híbrida aporta valor tangible.

Usar métricas claras como ahorro de costos, mejoras en tiempos de operación y eficiencia en recursos.

Provisión de soporte continuo:

Establecer equipos de apoyo dedicados para resolver dudas y facilitar el uso de las nuevas tecnologías.

Crear canales de comunicación abiertos para recibir y responder comentarios.

3. Formación y Capacitación

Programas de formación personalizada:

Diseñar cursos adaptados a las necesidades de diferentes grupos de usuarios (e.g., técnicos, administrativos, operativos).

Plataformas de aprendizaje: Implementar herramientas de e-learning y laboratorios prácticos para facilitar el aprendizaje progresivo.

4. Pruebas y Pilotos

Pilotos controlados: Implementar la tecnología en áreas específicas para medir la aceptación antes de una implementación masiva.

Feedback iterativo: Recopilar comentarios de los usuarios en cada etapa y ajustar la estrategia en consecuencia.

5. Comunicación Estratégica

Campañas de comunicación interna:

Explicar los objetivos y beneficios de la adopción híbrida de manera clara y accesible.

Compartir historias de éxito de usuarios que ya hayan adoptado la tecnología.

Promoción de champions tecnológicos: Identificar y capacitar a empleados clave que sirvan como embajadores de la adopción tecnológica.

6. Estrategias de Implementación

Segmentación de Usuarios

Identificar grupos con diferentes niveles de habilidad y actitud hacia la tecnología para diseñar estrategias específicas.

Priorizar a los usuarios con mayor impacto operativo para las primeras etapas de adopción.

Métricas de Éxito

Adopción inicial: Porcentaje de usuarios que comienzan a usar activamente la tecnología híbrida dentro de los primeros meses.

Satisfacción del usuario: Niveles de satisfacción recopilados a través de encuestas periódicas.

Impacto en el rendimiento: Incrementos en productividad, reducción de errores y mejoras en los tiempos de respuesta.

Soporte Continuo

Crear una mesa de ayuda especializada en tecnologías híbridas.

Implementar documentación accesible y actualizada que aborde problemas comunes.

7. Beneficios Esperados

Alta Tasa de Adopción:

Los usuarios adoptarán las tecnologías híbridas más rápidamente al percibir valor y facilidad de uso.

Reducción de Resistencias al Cambio:

Al abordar las preocupaciones y proveer formación adecuada, se minimizan las barreras psicológicas y culturales.

Mejora en el Desempeño:

Los usuarios trabajarán de manera más eficiente al aprovechar las capacidades de la nube pública y on-premise.

Satisfacción del Usuario:

Los empleados experimentarán mayor confianza y comodidad en el uso de las nuevas tecnologías.

Alineación Estratégica:

El uso efectivo de la tecnología híbrida estará alineado con los objetivos del negocio.

Análisis contexto situación Actual Anónima S.A.

Basándose en las perspectivas identificadas en el modelo CAF, se establece la siguiente relación de necesidades detectadas dentro de la organización:

Tabla 2

Perspectiva	Categoría	Acción	Descripción
Perspectiva de Negocio	Estrategia de TI	Gestión de consumo de clientes	Crear la capacidad de facturación dinámica con controles de consumo para los clientes.
Perspectiva de Negocio	Estrategia de TI	Creación de productos para disminuir el T2M (Time to Market)	Explotar los beneficios de agilidad, productividad y automatización para recortar los tiempos de creación de productos y su validación en el mercado.
Perspectiva de Negocio	Estrategia de TI	Transformación de oferta	Transformación de oferta de capacidad de cómputo (servidores) a servicio de valor agregado.
Perspectiva de Negocio	Estrategia de TI	Gestión de desarrollo de productos cloud	Definir la gestión de desarrollo de productos cloud que permita la generación de valor para cliente.
Perspectiva de Negocio	Finanzas de TI	Crear un modelo de negocio rentable y sostenible	Crear un modelo de negocio rentable y sostenible para Claro apalancado en los beneficios de aprovechamiento nube.
Perspectiva de Negocio	Realización de Beneficios	Generar la práctica de gestión de costos	Generar la práctica de gestión de costos para brindar al cliente optimización, control y proyección de costos.

Perspectiva de Personas	Gestión de Capacitación	Gestión de Planes de Capacitación por roles	Gestión de Planes de Capacitación por roles que incluya la participación en el modelo Claro desde venta hasta el soporte.
Perspectiva de Personas	Gestión de Capacitación	Planes de capacitación técnicos	Planes de capacitación técnicos que permitan el conocimiento del uso de herramientas de gestión de cloud.
Perspectiva de Personas	Gestión del Cambio Organizacional	Gestión de cambio en los servicios al cliente	Definir que la gestión del cambio incluya la transición a servicios de valor agregado basado en cloud.
Perspectiva de Personas	Gestión del Cambio Organizacional	Gestionar un plan de gestión del cambio organizacional	Gestión del cambio organizacional que identifique las áreas impactadas, su participación, entrenamientos y preparación a una nueva forma de operar.
Perspectiva de Personas	Gestión del Cambio Organizacional	Definición organización cloud que lidere la transición	Definición de estructura organizacional que lidere la transición con plan de comunicación al interior/exterior de Claro, ubicando las áreas nuevas y existentes y su interrelación.
Perspectiva de Personas	Gestión de Carrera	Definir nuevos modelos de capacitación	Definir nuevos modelos de capacitación en la iniciativa que permitan el desarrollo del personal en sus roles y planes de carrera.
Perspectiva de Gobernanza	Gestión de Programas y Proyectos	Organización de Suscripciones	Establecer una organización de gestión de suscripciones bajo las cuentas Claro o multi cuenta.
Perspectiva de Gobernanza	Gestión de Portafolio	Definir un portafolio de productos	Definir un portafolio de productos que permita la innovación de servicios para clientes internos y externos.
Perspectiva de Gobernanza	Gestión de Programas y Proyectos	Establecer plan de mejora continua	Establecer mecanismos de mejora continua a los productos, cliente y desarrollo de recursos Claro.
Perspectiva de Gobernanza	Medición del Desempeño Empresarial	Gestión para asegurar cumplimientos	Asegurar cumplimientos en SLA, SLO, estándares corporativos y acuerdos con terceros.
Perspectiva de Gobernanza	Gestión de Portafolio	Respaldo de iniciativa Cloud Pública	Desarrollo de Caso de Negocio de iniciativa Cloud Pública ante stakeholder corporativos.
Perspectiva de Gobernanza	Gestión de Programas y Proyectos	Establecer una organización ágil	Establecer una organización ágil que permita la interacción entre áreas, grupos o células en el modelo operacional.

Perspectiva de Plataforma	Aprovisionamiento de Cómputo	Definir procesos de aprovisionamiento	Definir procesos de aprovisionamiento gestionados en tiempo, diversidad en nubes (públicas y privadas).
Perspectiva de Plataforma	Aprovisionamiento de Redes	Automatización en aprovisionamiento de redes	Automatización en aprovisionamiento de redes incluido como servicios de Cloud.
Perspectiva de Plataforma	Arquitectura de Sistemas y Soluciones	Establecer práctica de migración	Establecer práctica que desarrolle procesos de migración, operaciones híbridas y automatización de operaciones.
Perspectiva de Plataforma	Arquitectura de Sistemas y Soluciones	Modelo de soluciones internas y externas	Establecer una práctica de consultoría que permita desarrollar soluciones particulares y estándares.
Perspectiva de Seguridad	Gestión de Identidad y Acceso	Establecer plan de entrenamiento para seguridad	Establecer plan de entrenamiento para seguridad como proceso integral, herramientas y responsabilidades.
Perspectiva de Seguridad	Control Detectivo	Desarrollar práctica de seguridad de cumplimiento	Desarrollar práctica de seguridad de cumplimiento de regulaciones de sector, industria y corporativa.
Perspectiva de Seguridad	Control Detectivo	Desarrollar Gestión de fraudes	Como práctica complementaria de seguridad, habilitar los servicios de antifraude, cumplimiento continuo y seguridad por diseño.
Perspectiva de Seguridad	Protección de Datos	Desarrollar modelo de responsabilidad compartida	Desarrollar modelo que permita establecer roles, funciones, accesos y controles a los clientes de su manejo de información.
Perspectiva de Seguridad	Respuesta a Incidentes	Establecer una práctica de seguridad	Establecer una práctica de seguridad dentro de la organización Claro Cloud que desarrolle los modelos de responsabilidad, controles y roles.
Perspectiva de Operaciones	Gestión de Liberaciones / Gestión del Cambio	Definir procesos de gestión de cambio ágiles	Definir procesos de gestión de cambio ágiles gobernados para no recrear prácticas tradicionales.
Perspectiva de Operaciones	Monitoreo del Rendimiento de Aplicaciones	Evitar vendor Lock-in	Establecer estrategia que evite dependencia de fabricante ante problemas críticos.
Perspectiva de Operaciones	Continuidad del Negocio / Recuperación ante Desastres	Servicios con BCP y DR	Incluir desde diseño características de BCP y DR como oferta de valor a los clientes.

Perspectiva de Operaciones	Monitoreo de Servicios	Creación de Modelo de Operación multi-nube y privado	Crear capacidad de administración, monitoreo, gestión de incidentes y escalamientos multicloud.
Perspectiva de Operaciones	Informes y Análisis	Herramientas analíticas	Herramientas analíticas transversales para gestión correlacional multi-nube.

Propuesta

Con base en el análisis y resultados de investigación y las conclusiones presentadas se propone el siguiente modelo de operación fundacional para la operación de las plataformas y subscripciones de cloud públicas en Anónima S.A.:

Anónima S.A. enfrenta desafíos significativos al gestionar su modelo de operación de TI actual, basado en una infraestructura on-premises y estructuras organizacionales en silos. Estas limitaciones afectan la eficiencia operativa, la capacidad de respuesta a las demandas del negocio y la integración con tecnologías avanzadas en entornos híbridos.

Con base en el análisis realizado, se han identificado oportunidades clave para transformar la operación de las plataformas y suscripciones en la nube pública mediante un modelo fundacional adaptado a las necesidades específicas de Anónima S.A. Este modelo tiene como objetivo establecer un marco estratégico que permita gestionar de manera eficiente, escalable y segura los recursos en la nube, aprovechando las mejores prácticas y marcos de trabajo reconocidos, como ITIL, el Cloud Adoption Framework (CAF) y principios de automatización como Infrastructure as Code (IaC).

Equipos de Trabajo Clave:

La propuesta incluye la conformación de tres equipos especializados que operarán en conjunto para garantizar el éxito del modelo fundacional de operación en la nube:

Cloud Business Team

Este equipo será responsable de alinear las necesidades del negocio con las capacidades tecnológicas en la nube. Sus funciones incluyen:

- Identificación de casos de uso estratégicos para la nube.
- Gestión de suscripciones y optimización de costos.
- Análisis y monitoreo del retorno de inversión (ROI) de las iniciativas en la nube.
- Promoción de la adopción de tecnologías cloud mediante programas de capacitación y gestión del cambio.

Cloud Platform Operations Team

Este equipo gestionará las operaciones diarias de las plataformas en la nube, asegurando la continuidad del negocio y la eficiencia operativa. Sus responsabilidades abarcan:

- Monitoreo proactivo de servicios utilizando herramientas como Azure Monitor, AWS CloudWatch, entre otras.
- Gestión de incidentes y recuperación ante desastres (DR).
- Implementación de políticas de gobernanza automatizada para garantizar cumplimiento normativo y seguridad.
- Coordinación con equipos de desarrollo para garantizar la integración continua (CI/CD) en entornos híbridos.

Cloud Platform Infrastructure Team

Este equipo se encargará de diseñar, implementar y mantener la infraestructura técnica necesaria para la operación de las plataformas en la nube. Sus actividades clave incluyen:

- Implementación y gestión de landing zones seguras y escalables.
- Automatización de la infraestructura mediante herramientas como Terraform, Ansible y AWS CloudFormation.
- Configuración y optimización de redes, bases de datos y almacenamiento en la nube.
- Garantizar altos niveles de disponibilidad y rendimiento mediante la adopción de arquitecturas resilientes.

Objetivo General de la Propuesta

El objetivo del modelo fundacional es establecer un marco operativo que permita a Anónima S.A. gestionar eficientemente sus plataformas y suscripciones en la nube pública, garantizando la seguridad, la escalabilidad y la optimización de costos, mientras se fomenta la colaboración multidisciplinaria y la transformación organizacional.

Tabla 3

Equipo Cloud de Negocio - Modelo Operativo Cloud Hibrido - Objetivos

Cloud Business Team	
Objetivos	Impulsar una adopción efectiva de la nube que esté alineada con los objetivos del negocio, optimice los recursos financieros, garantice la seguridad y el cumplimiento, fomente la innovación y la agilidad, y promueva la colaboración y el desarrollo de habilidades dentro de la organización.
	Alinear la estrategia de la nube con los objetivos del negocio: Asegurar que la estrategia de adopción de la nube esté alineada con los objetivos generales del negocio y que la inversión en la nube genere un valor real y medible para la organización.
	Gestionar eficientemente los recursos financieros: Uno de los objetivos principales es el de garantizar que los recursos financieros invertidos en la adopción de la nube se utilicen de manera eficiente y se maximice el retorno de la inversión (ROI). Esto incluye la optimización de costos, la gestión del presupuesto y la transparencia en el gasto en la nube.
	Garantizar la seguridad y el cumplimiento: Establecer políticas, procesos y controles para garantizar la seguridad y el cumplimiento de los datos y los recursos en la nube. Esto implica implementar medidas de seguridad robustas y cumplir con los estándares y regulaciones de la industria.
	Fomentar la innovación y la agilidad: Fomentar una cultura de innovación y agilidad dentro de la organización, impulsando la adopción de prácticas y tecnologías modernas en la nube que permitan a la organización responder rápidamente a las demandas del mercado y a las oportunidades emergentes.
	Facilitar la colaboración y la comunicación: Facilitador de la colaboración y la comunicación entre diferentes equipos y partes interesadas dentro de la organización, asegurando una alineación efectiva y un enfoque colectivo hacia la adopción de la nube.
	Promover la gestión del cambio y el desarrollo de habilidades: Promueve la gestión del cambio y el desarrollo de habilidades necesarias para trabajar en entornos en la nube, facilitando la formación y la capacitación adecuadas para los empleados y promoviendo una cultura de aprendizaje continuo.

Tabla 4

Equipo Cloud de Negocio - Modelo Operativo Cloud Hibrido – Roles y Funciones

Cloud Business Team		
Funciones	**Estrategia de Negocio Multi-Cloud**	**Definición del catálogo de servicios Multi-cloud:** Colabora con las partes interesadas para identificar y definir los servicios en la nube que la organización ofrecerá a sus clientes internos o externos. Esto implica comprender las necesidades del mercado, evaluar las capacidades internas y definir una cartera de servicios que agregue valor a los clientes y al negocio.
		Priorización de características y funcionalidades: Prioriza las características y funcionalidades de los servicios en la nube en función de las necesidades del cliente, el valor comercial y la viabilidad técnica. Esto implica colaborar con los equipos de desarrollo y otras partes interesadas para establecer una hoja de ruta clara y gestionar las expectativas de los clientes.
		Definición de requisitos y especificaciones: Trabaja con los clientes y las partes interesadas para definir los requisitos y especificaciones de los servicios en la nube. Esto implica capturar y documentar los requisitos del cliente, elaborar historias de usuarios y definir criterios de aceptación para garantizar que los servicios cumplen con las expectativas del cliente.
		Análisis de mercado y competencia: Realiza análisis de mercado y de la competencia para identificar tendencias emergentes, evaluar la posición de la organización en el mercado y encontrar oportunidades para diferenciarse. Esto implica monitorear de cerca el mercado, realizar análisis comparativos y recopilar información sobre las prácticas de la competencia.
		Gestión del ciclo de vida de los productos: Gestiona el ciclo de vida completo de los servicios en la nube, desde la concepción hasta el lanzamiento y más allá. Esto implica la planificación de lanzamientos, la gestión de actualizaciones y mejoras, y la retirada de servicios obsoletos o no rentables.
	Arquitectura Empresarial Multi-Cloud	**Análisis de requisitos técnicos:** Comprender en profundidad los requisitos técnicos de los proyectos y las soluciones en la nube que se van a implementar. Esto implica colaborar estrechamente con los equipos de proyecto y los interesados para identificar y comprender los requisitos técnicos específicos.
		Descomposición del trabajo técnico: Descomponer el trabajo técnico en tareas y actividades más pequeñas y manejables, que puedan ser abordadas de manera efectiva por los equipos de desarrollo y los arquitectos técnicos. Esto implica dividir el trabajo en componentes lógicos y definir las interacciones y dependencias entre ellos.

		Definición de la arquitectura de soluciones: Utilizar la descomposición del trabajo técnico como base para definir la arquitectura de las soluciones en la nube. Esto implica diseñar la estructura de las aplicaciones, los servicios y los recursos en la nube de manera que satisfagan los requisitos técnicos y las necesidades del negocio.
		Validación y revisión de la arquitectura: Revisar y validar la arquitectura propuesta para asegurar que esté alineada con la descomposición del trabajo técnico y cumpla con los requisitos y estándares técnicos establecidos. Identificar y abordar posibles desviaciones o áreas de mejora en la arquitectura propuesta.
		Asegurar la coherencia y consistencia: Garantizar que la arquitectura de las soluciones en la nube sea coherente y consistente con la descomposición del trabajo técnico, así como con las directrices arquitectónicas y los estándares de la organización. Esto implica mantener una comunicación efectiva y colaborar con los equipos de proyecto y los arquitectos técnicos para asegurar la alineación.
		Gestión del cambio y la evolución: Adaptar la arquitectura de las soluciones en la nube según sea necesario para satisfacer los requisitos cambiantes del negocio y los avances tecnológicos. Esto implica gestionar el cambio de manera efectiva y asegurar que la arquitectura evolucione de manera coherente y sostenible con el tiempo.
	Gestión Financiera Multi-Cloud	**Planificación de costos y presupuestos:** Colabora en la planificación de costos y la elaboración de presupuestos para la adopción de la nube. Esto implica estimar los costos asociados con la migración a la nube, la implementación de servicios en la nube y la operación continua en la nube, así como asignar presupuestos apropiados para cada fase del proyecto.
		Análisis de costos y optimización: Realizar análisis detallados de los costos de la nube y buscar oportunidades para optimizar el gasto. Esto puede incluir la identificación de recursos subutilizados, la eliminación de costos innecesarios, la optimización de la capacidad y el uso de modelos de precios más rentables.
		Seguimiento y gestión del gasto: Seguir de cerca el gasto en la nube y gestionar los presupuestos asignados para garantizar que se mantengan dentro de los límites establecidos. Esto implica monitorear los costos en tiempo real, identificar desviaciones y tomar medidas correctivas cuando sea necesario.
		Gestión de facturación y pagos: Gestionar el proceso de facturación y pagos relacionados con los servicios en la nube. Esto implica garantizar la precisión de las facturas, optimizar los métodos de pago y gestionar los acuerdos de facturación con los proveedores de servicios en la nube.

		Establecimiento de políticas y controles financieros: Desarrollar políticas y controles financieros para garantizar el cumplimiento y la transparencia en la gestión del gasto en la nube. Esto puede incluir establecer políticas de aprovisionamiento, límites de gasto y controles de acceso a recursos en la nube.
		Análisis de rentabilidad y ROI: Realizar análisis de rentabilidad y retorno de la inversión (ROI) para evaluar el valor generado por la adopción de la nube. Esto implica comparar los costos con los beneficios obtenidos y proporcionar informes y análisis para respaldar la toma de decisiones.
		Asesoramiento y recomendaciones: Proporcionar asesoramiento y recomendaciones a los líderes de la organización sobre estrategias para optimizar el gasto en la nube y maximizar el valor de la inversión. Esto puede incluir la identificación de áreas de mejora, la evaluación de opciones de licenciamiento y la recomendación de mejores prácticas financieras.
	Gestión de Implementación Multi-Cloud	**Planificación y programación de entregas:** Colaborar con los equipos de proyecto y las partes interesadas para desarrollar planes detallados de entregas y cronogramas para la adopción de la nube. Esto implica definir los hitos, establecer objetivos y asignar recursos de manera eficiente para garantizar la entrega oportuna de los proyectos.
		Gestión de recursos y capacidades: Gestionar los recursos y capacidades necesarios para llevar a cabo las iniciativas de adopción de la nube. Esto incluye la asignación de personal, la gestión de proveedores externos y la coordinación de equipos multidisciplinarios para garantizar que se cumplan los requisitos de recursos y se optimice el rendimiento del equipo.
		Monitoreo y seguimiento del progreso: Supervisar el progreso de las entregas en curso y realizar un seguimiento de los hitos y los objetivos establecidos. Esto implica identificar y abordar los riesgos y problemas potenciales que puedan surgir durante la ejecución de los proyectos y tomar medidas correctivas según sea necesario para garantizar el éxito de la entrega.
		Gestión del riesgo y la calidad: Identificar, evaluar y gestionar los riesgos asociados con las iniciativas de adopción de la nube, así como garantizar la calidad de los entregables y resultados. Esto puede incluir la implementación de procesos de gestión de riesgos, la realización de pruebas de calidad y la implementación de controles de calidad para garantizar que los proyectos cumplan con los estándares y requisitos definidos.
		Comunicación y colaboración: Facilitar la comunicación efectiva y la colaboración entre los diferentes equipos, partes interesadas y socios involucrados en las iniciativas de adopción de la nube. Esto implica mantener a todas las partes informadas sobre el progreso, los cambios y los problemas, y fomentar un ambiente de trabajo colaborativo y transparente.

		Gestión del cambio: Apoyar la gestión del cambio organizacional asociado con la adopción de la nube, ayudando a los equipos y las partes interesadas a adaptarse a nuevos procesos, herramientas y formas de trabajo. Esto puede incluir la planificación y ejecución de actividades de capacitación, comunicación y apoyo para garantizar una transición suave y exitosa.
		Evaluación y mejora continua: Realizar evaluaciones periódicas de las entregas y los procesos de entrega para identificar oportunidades de mejora y optimización. Esto implica recopilar y analizar retroalimentación, métricas de desempeño y lecciones aprendidas para impulsar la mejora continua y la eficiencia en la ejecución de proyectos futuros.
	Integración de Clientes Multi-Cloud	**Comunicación y Educación:** Proporcionar información clara y detallada sobre los servicios en la nube, incluyendo características, beneficios, requisitos y procedimientos de uso. Esto puede incluir la creación de materiales educativos, guías de usuario y tutoriales.
		Configuración y Provisionamiento: Ayudar a los clientes a configurar y aprovisionar sus cuentas y recursos en la nube de acuerdo con sus necesidades y requisitos específicos. Esto puede incluir la asistencia en la configuración inicial, la asignación de recursos y la personalización de la plataforma.
		Formación y Capacitación: Proporcionar formación y capacitación adecuadas sobre el uso de los servicios en la nube. Esto puede incluir sesiones de formación en persona, webinars, documentación detallada y recursos de autoaprendizaje.
		Soporte y Asistencia: Ofrecer soporte técnico y asistencia en caso de problemas o preguntas relacionadas con el uso de los servicios en la nube. Esto puede incluir la resolución de problemas técnicos, la respuesta a consultas de usuarios y la coordinación con otros equipos de soporte técnico.
		Seguimiento y Retroalimentación: Realizar un seguimiento de la experiencia del cliente durante el proceso de integración y recopilar retroalimentación para identificar áreas de mejora. Esto puede incluir encuestas de satisfacción del cliente, entrevistas y análisis de datos de uso.
		Optimización y Mejora Continua: Identificar oportunidades para optimizar y mejorar el proceso de integración del cliente en curso. Esto puede incluir la automatización de tareas, la simplificación de procesos y la implementación de nuevas funcionalidades o características basadas en la retroalimentación del cliente.
	Gestión de Capacitación y Desarrollo	**Desarrollo de programas de capacitación:** Diseña y desarrolla programas de capacitación adaptados a las necesidades específicas de la organización en relación con la adopción de la nube. Esto puede incluir cursos presenciales, sesiones virtuales, materiales de capacitación en línea, tutoriales y otros recursos educativos.

		Identificación de necesidades de capacitación: Colabora con los líderes de la organización y los equipos involucrados en la adopción de la nube para identificar las áreas en las que se requiere capacitación adicional. Esto puede implicar la evaluación de habilidades actuales, la identificación de brechas de conocimiento y la determinación de necesidades de desarrollo profesional.
		Entrenamiento técnico: Proporcionar capacitación técnica sobre herramientas, plataformas y servicios en la nube específicos que se están implementando o utilizando en la organización. Esto puede incluir formación sobre plataformas de infraestructura como servicio (IaaS), software como servicio (SaaS), plataformas de contenedores, entre otros.
		Entrenamiento en mejores prácticas y metodologías: Capacitar a los empleados en las mejores prácticas y metodologías relacionadas con la adopción de la nube, como DevOps, Agile, gestión de proyectos en la nube, seguridad en la nube, gobernanza en la nube, entre otros.
		Facilitación de talleres y sesiones de capacitación: Organizar y facilitar talleres y sesiones de capacitación para equipos específicos o grupos de empleados. Esto puede incluir sesiones prácticas, ejercicios de simulación, estudios de caso y actividades de aprendizaje colaborativo.
		Evaluación y seguimiento del progreso: Evaluar el progreso y el impacto de la capacitación realizada, recopilando retroalimentación de los participantes y realizando evaluaciones periódicas de habilidades y competencias adquiridas. Esto ayuda a identificar áreas de mejora y a garantizar la efectividad de los programas de capacitación.
		Mentoría y apoyo individualizado: Proporcionar mentoría y apoyo individualizado a empleados que requieran asistencia adicional en el desarrollo de habilidades relacionadas con la adopción de la nube. Esto puede incluir sesiones de tutoría, asesoramiento personalizado y seguimiento continuo.
		Actualización y adaptación continua: Mantenerse actualizado sobre las últimas tendencias y desarrollos en tecnologías en la nube y en prácticas de capacitación, ajustando y actualizando los programas de capacitación según sea necesario para garantizar su relevancia y efectividad.
	Gestión de Cambio Organizacional	**Desarrollo de estrategias de cambio:** Desarrollar estrategias y planes de cambio adaptados a las necesidades y características específicas de la organización, incluyendo la comunicación, la capacitación, la participación de los empleados y la gestión de resistencias.
		Comunicación y concienciación: Crear y ejecutar planes de comunicación para informar a los empleados sobre los cambios relacionados con la adopción de la nube, así como para generar conciencia sobre los beneficios y objetivos del cambio.
		Gestión de resistencias: Identificar y gestionar las resistencias al cambio que puedan surgir dentro de la organización, abordando las preocupaciones de los empleados, fomentando la participación y promoviendo una cultura de apoyo al cambio.

		Facilitación de equipos de trabajo y grupos de interés: Facilitar reuniones, talleres y sesiones de trabajo con equipos y grupos de interés clave para fomentar la colaboración, la participación y la resolución de problemas relacionados con el cambio.
		Medición del progreso y ajuste de estrategias: Medir el progreso de la implementación del cambio y ajustar las estrategias según sea necesario para abordar desafíos y garantizar el éxito continuo del proceso de adopción de la nube.
		Cultura y liderazgo organizacional: Fomentar una cultura organizacional que apoye la innovación, la colaboración y la adaptabilidad, así como identificar y desarrollar líderes que puedan guiar y respaldar el cambio dentro de la organización.

Tabla 5

Equipo de Operación Plataforma Cloud - Modelo Operativo Cloud Hibrido – Objetivos

Cloud Platform Operation Team	
Objetivos	Facilitar la gestión eficaz y continua de la infraestructura y servicios en la nube, asegurando la disponibilidad, rendimiento, seguridad y eficiencia operativa para satisfacer las necesidades del negocio. Esto implica la implementación de prácticas de operaciones estandarizadas, automatización de tareas, monitorización proactiva, gestión de incidentes y colaboración con otros equipos y proveedores de servicios. El objetivo es optimizar el uso de recursos, mitigar los riesgos y garantizar que la infraestructura en la nube respalde de manera efectiva los objetivos estratégicos de la organización.
	Garantizar la disponibilidad y confiabilidad de los servicios en la nube: Asegurar que los servicios en la nube estén disponibles y funcionen de manera confiable para satisfacer las necesidades operativas y comerciales de la organización.
	Optimizar el rendimiento de los servicios en la nube: Mejorar el rendimiento de los servicios en la nube para garantizar tiempos de respuesta rápidos y eficientes, y proporcionar una experiencia óptima a los usuarios finales.
	Mantener la seguridad de los servicios en la nube: Implementar y mantener controles de seguridad adecuados para proteger los datos y los recursos en la nube contra amenazas de seguridad, vulnerabilidades y ataques cibernéticos.
	Gestionar eficientemente los costos de la nube: Optimizar el uso de recursos en la nube para reducir los costos operativos y maximizar el retorno de la inversión en la adopción de la nube.
	Automatizar y estandarizar las operaciones en la nube: Implementar prácticas de automatización y estandarización para simplificar y agilizar las operaciones en la nube, reducir el error humano y mejorar la eficiencia operativa.
	Monitorizar y gestionar el rendimiento de la nube: Monitorizar de forma proactiva el rendimiento de los servicios en la nube y gestionar los recursos según sea necesario para optimizar el rendimiento y la disponibilidad de los servicios.
	Gestionar el cambio y la configuración en la nube: Gestionar eficazmente los cambios y la configuración en la nube para garantizar la estabilidad y la integridad de los servicios en la nube, y minimizar los riesgos asociados con cambios no autorizados.
	Promover la mejora continua: Identificar oportunidades de mejora en las operaciones en la nube y promover la adopción de mejores prácticas para garantizar un funcionamiento eficiente y efectivo de los servicios en la nube.

Tabla 6

Equipo de Operación Plataforma Cloud - Modelo Operativo Cloud Hibrido – Roles y Funciones

Cloud Platform Operation Team			
Funciones	Plataforma	**Modelos de Implementación Automatizada**	**Automatización de Implementación de Enterprise Stacks:** Desarrollar scripts y herramientas de automatización para desplegar y configurar Enterprise Stacks de manera consistente y confiable en diferentes entornos de la nube.
			Desarrollo y Mantenimiento de Enterprise Stacks: Colaborar con equipos de arquitectura y desarrollo para diseñar, desarrollar y mantener Enterprise Stacks (conjuntos de recursos y configuraciones estandarizadas) que representen patrones codificados para implementaciones empresariales comunes.
			Gestión de Configuración: Implementar y mantener herramientas de gestión de configuración para administrar y controlar las configuraciones de los Enterprise Stacks, garantizando la coherencia y la integridad en todos los entornos de la nube.
			Optimización de Primitives: Identificar, desarrollar y mantener primitives (elementos básicos de configuración y recursos) que sirvan como componentes reutilizables en los Enterprise Stacks, optimizando su eficiencia y flexibilidad.
			Integración con Configuration Management Tools: Integrar los Enterprise Stacks con herramientas de gestión de configuración para automatizar y simplificar la implementación, configuración y mantenimiento de la infraestructura en la nube.
			Documentación y Capacitación: Documentar los Enterprise Stacks, primitives y procesos relacionados, y proporcionar capacitación y soporte técnico a otros equipos en su uso y mantenimiento.
			Mejora Continua: Analizar y optimizar los Enterprise Stacks y primitives existentes para mejorar la eficiencia operativa, el rendimiento y la seguridad de la infraestructura en la nube, y buscar constantemente formas de mejorar y evolucionar los patrones codificados.
		Administración de Plataforma Cloud	**Networking y Seguridad:** Diseño e implementación de la infraestructura de red necesaria para admitir servicios en la nube, incluida la configuración de redes virtuales, subredes, enrutamiento y seguridad de red. Implementación de prácticas de conectividad segura entre servicios y aplicaciones en la nube, como el uso de VPNs, VPC peering o servicios de gateway. Configuración y mantenimiento de servicios de Load Balancer, CDN y DNS para optimizar el rendimiento y la disponibilidad de las aplicaciones en la nube. Configuración de segmentación de red y aislamiento para garantizar la separación de cargas de trabajo y aplicaciones dentro de la Landing Zone.

			Cuentas de Usuario: Gestión y configuración de cuentas de usuario y grupos en la nube, asegurando la correcta asignación de permisos y acceso a los recursos. Implementación de políticas y procedimientos para la creación, modificación y eliminación segura de cuentas de usuario y grupos. Automatización de tareas administrativas relacionadas con la gestión de cuentas, como la provisión de nuevas cuentas y la gestión de permisos.
			Identidad y Acceso (IAM): Diseño e implementación de políticas de seguridad y control de acceso para proteger los recursos en la nube y garantizar el cumplimiento de los requisitos de seguridad. Configuración de roles, políticas y permisos para gestionar el acceso a los recursos de manera granular y basada en el principio de menor privilegio. Integración con servicios de directorio existentes y soluciones de gestión de identidad para centralizar la gestión de identidades y facilitar la autenticación y autorización.
			Integración SSO: Integración con proveedores de identidad externos para permitir la autenticación de usuarios utilizando sus credenciales existentes. Implementación de soluciones de Single Sign-On (SSO) para proporcionar un acceso unificado y seguro a los servicios y recursos dentro de la Landing Zone. Gestión de grupos y políticas asignadas a la integración de plataformas SSO.
	Operaciones	**Desarrollo, Pruebas y Despliegue de Servicios**	**Automatización de Pruebas y Despliegue:** Desarrollar y mantener pipelines de CI/CD para automatizar el proceso de pruebas y despliegue de servicios y aplicaciones en la nube. Administrar e Integrar herramientas de desarrollo, pruebas y despliegue en pipelines automatizados para garantizar la entrega rápida y confiable de los servicios a desplegar en la nube.
			Integración Continua y Entrega Continua (CI/CD): Configurar y administrar herramientas de CI/CD para automatizar la integración continua, las pruebas automáticas y el despliegue continuo de cambios de código y artefactos de automatización. Establecer prácticas de integración y entrega continua para acelerar el ciclo de desarrollo y mejorar la calidad de los despliegues de servicios en la nube.
			Gestión de Versiones y Despliegues: Planificar y coordinar los despliegues de servicios y/o plataformas, asegurando que los cambios se implementen de manera controlada y se puedan revertir si es necesario. Gestionar versiones de códigos y artefactos de automatización del despliegue, manteniendo un registro histórico de cambios y asegurando la trazabilidad y la integridad del código fuente y los artefactos.
			Gestión de Configuración: Automatizar la configuración de infraestructura y aplicaciones utilizando herramientas de gestión de configuración como Ansible o Terraform, o la integración entre ellas. Establecer políticas y estándares de configuración para garantizar la coherencia y la integridad de la configuración de los servicios y plataformas en la nube.

			Gestión del Código Fuente y Artefactos: Gestionar repositorios de código fuente y artefactos de software utilizando sistemas de control de versiones como Git, GitLab, GitHub, Ansible Automation Platform o Terraform Cloud. Establecer prácticas de gestión de código fuente y artefactos para facilitar la colaboración, la revisión de código y el control de versiones.
		Gestión y Operación de Plataformas y Servicios	**Monitorización y Gestión de la disponibilidad de Servicios de Nube:** Supervisar el estado y el rendimiento de la infraestructura y los servicios en la nube, utilizando herramientas de monitorización para identificar y resolver problemas de manera proactiva.
			Gestión de Incidentes y Problemas: Gestionar y resolver incidentes y problemas operativos en la nube, siguiendo procesos definidos para minimizar el impacto en las operaciones del negocio.
			Gestión de Cambios: Planificar, coordinar y controlar cambios en la infraestructura y los servicios en la nube, asegurando que se realicen de manera controlada y minimizando el riesgo de interrupciones.
			Seguridad y Cumplimiento: Implementar y mantener controles de seguridad para proteger la infraestructura y los datos en la nube, y garantizar el cumplimiento de los requisitos de seguridad y regulaciones aplicables.
			Optimización de Costos: Analizar y optimizar el uso de recursos en la nube para minimizar los costos operativos, identificando áreas de mejora y aplicando prácticas de optimización de costos.
			Gestión de Capacidades: Gestionar y planificar la capacidad de la infraestructura en la nube para garantizar que pueda satisfacer las demandas actuales y futuras de las cargas de trabajo.
			Respaldo y Recuperación: Establecer y mantener procesos de respaldo y recuperación de datos para proteger contra la pérdida de datos y garantizar la continuidad del negocio en caso de desastres.
			Planificación, Evaluación e Implementación de Actualizaciones y Parches: Desarrollar y mantener un plan de actualización y parcheo que identifique los sistemas y servicios que requieren actualizaciones, así como el cronograma para implementarlas. Evaluar la criticidad y el impacto potencial de los parches antes de aplicarlos, incluyendo pruebas en entornos de prueba para asegurar la compatibilidad y estabilidad del sistema. Implementar parches de seguridad y actualizaciones de software en la infraestructura y los servicios de manera oportuna y eficiente, minimizando el tiempo de inactividad y el impacto en las operaciones.

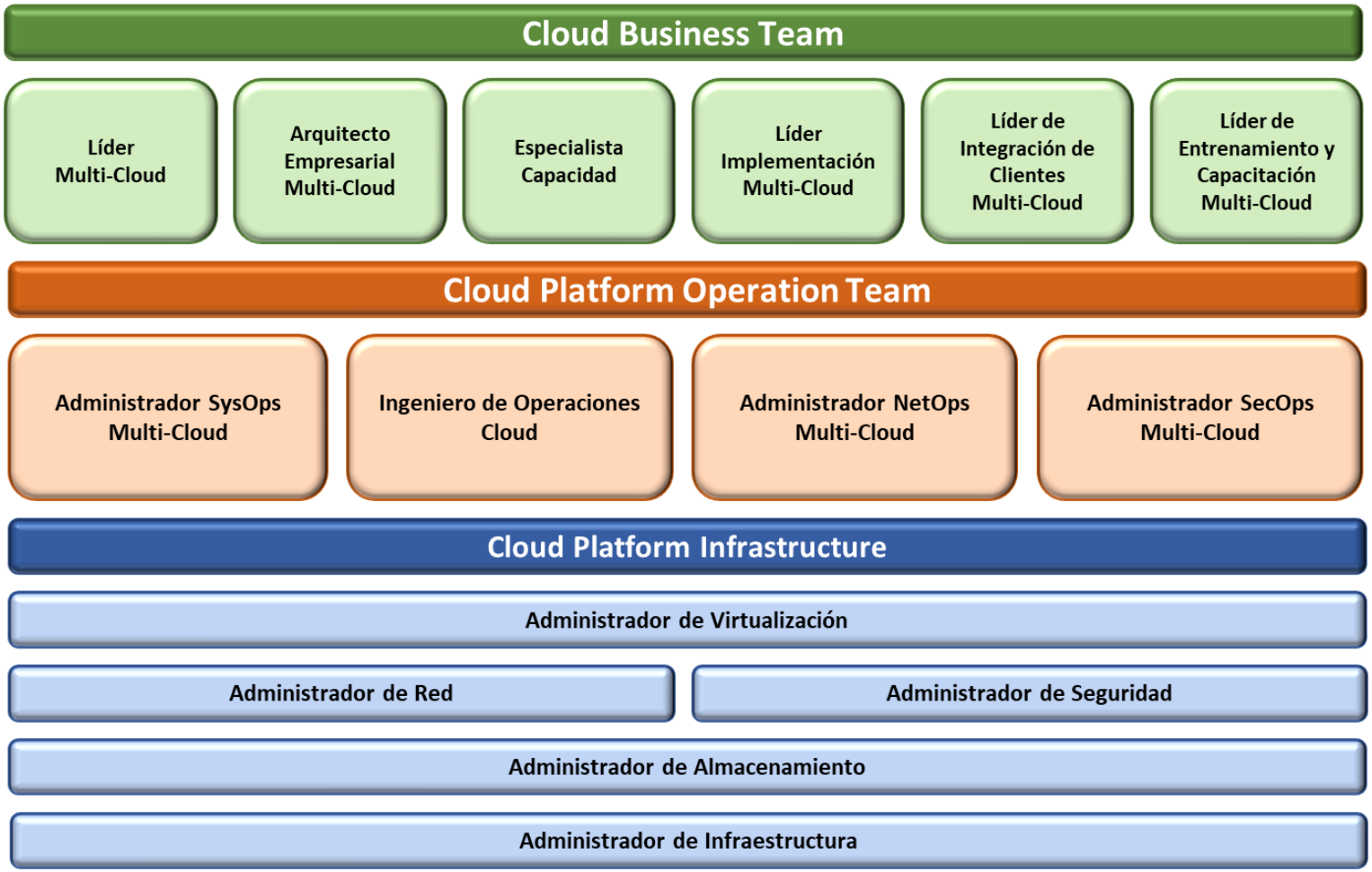
			Gestión de Identidad y Acceso: Configurar y gestionar la autenticación y autorización de usuarios y servicios en la nube, asegurando que tengan acceso apropiado a los recursos.
			Automatización y Orquestación: Desarrollar y mantener procesos de automatización y orquestación para simplificar y agilizar las operaciones en la nube, maximizando la eficiencia operativa. Automatizar procesos de actualización y parches siempre que sea posible, utilizando herramientas y scripts para agilizar el proceso y reducir la posibilidad de errores humanos.
	Seguridad	**Definición y Aplicación de políticas y controles de seguridad**	**Definición de Políticas de Seguridad:** Colaborar con los equipos de seguridad y cumplimiento para definir políticas de seguridad claras y efectivas que aborden los requisitos de seguridad de la organización y las regulaciones aplicables.
			Desarrollo de Controles de Seguridad: Diseñar y desarrollar controles de seguridad técnicos y procesos operativos para proteger la infraestructura y los datos en la nube contra amenazas y vulnerabilidades.
			Implementación de Controles de Seguridad: Implementar y configurar controles de seguridad en la infraestructura y los servicios en la nube, utilizando herramientas y servicios nativos de la nube, así como soluciones de terceros si es necesario.
			Gestión de Identidad & Acceso y Gestión de Políticas: Diseñar y mantener políticas de acceso basadas en roles (RBAC) para controlar el acceso a los recursos en la nube en función de los roles y responsabilidades de los usuarios. Configurar y gestionar la autenticación multifactor (MFA) y otros controles de autenticación para fortalecer la seguridad de las cuentas de usuario. Implementar políticas de acceso granular a través de la gestión de políticas de acceso (IAM Policies) para restringir el acceso a recursos específicos en función de las necesidades del negocio y los principios de menor privilegio.
			Seguridad de Red: Configurar y gestionar listas de control de acceso (ACL) y grupos de seguridad para controlar el tráfico de red dentro de la infraestructura en la nube y entre los servicios. Implementar segmentación de red y zonas de seguridad para aislar y proteger los recursos críticos y sensibles de la infraestructura. Utilizar herramientas de detección y prevención de intrusiones (IDS/IPS) para monitorear y proteger la red contra ataques y actividades maliciosas.

			Secretos y Encripción: Implementar prácticas de gestión de secretos para proteger información confidencial, como contraseñas, claves API y certificados digitales. Utilizar servicios de gestión de claves (KMS) para generar, almacenar y gestionar claves de cifrado utilizadas para proteger datos sensibles en reposo y en tránsito. Encriptar datos sensibles tanto en reposo como en tránsito utilizando algoritmos de cifrado robustos y certificados de seguridad adecuados.
			Auditoría y Cumplimiento: Realizar auditorías periódicas de seguridad para evaluar el cumplimiento de las políticas y controles de seguridad, y proporcionar informes y evidencia de cumplimiento a las partes interesadas internas y externas.
			Automatización de Seguridad: Automatizar procesos y controles de seguridad siempre que sea posible, utilizando herramientas de automatización para garantizar la consistencia y eficacia de la aplicación de políticas de seguridad.
		Detección y Respuesta a Incidentes	**Gestión de Amenazas y Vulnerabilidades:** Realizar evaluaciones periódicas de riesgos y vulnerabilidades en la infraestructura y los servicios en la nube para identificar posibles amenazas y puntos de vulnerabilidad. Utilizar herramientas y técnicas de escaneo de vulnerabilidades para detectar y evaluar posibles vulnerabilidades en la infraestructura y las aplicaciones en la nube. Priorizar y remediar las vulnerabilidades identificadas mediante la implementación de parches, actualizaciones de seguridad y otras medidas correctivas.
			SIEM - Gestión de Información y Eventos de Seguridad: Implementar y configurar una plataforma SIEM (Security Information and Event Management) para recopilar, correlacionar y analizar eventos de seguridad de múltiples fuentes en la infraestructura en la nube. Monitorear continuamente los eventos de seguridad en busca de indicadores de compromiso y patrones de actividad maliciosa que puedan indicar una amenaza. Configurar alertas y notificaciones automáticas para advertir sobre eventos de seguridad sospechosos o anomalías que requieran una acción inmediata.
			Respuesta a Incidentes y Forense: Desarrollar y mantener un plan de respuesta a incidentes que detalle los roles, responsabilidades y procedimientos para manejar incidentes de seguridad en la nube. Responder rápidamente a los incidentes de seguridad identificados, investigando la causa raíz, evaluando el alcance del impacto y tomando medidas correctivas para mitigar el daño. Realizar análisis forenses de incidentes de seguridad para recopilar evidencia, reconstruir eventos y facilitar la atribución de amenazas a actores maliciosos.

	Contención y Erradicación: Implementar medidas para contener y erradicar la amenaza, como la eliminación de malware, el restablecimiento de contraseñas comprometidas y la restauración de sistemas afectados a un estado seguro.
	Notificación y Reporte: Notificar a las partes interesadas internas y externas sobre incidentes de seguridad, proporcionando informes detallados sobre la naturaleza del incidente, las acciones tomadas y las lecciones aprendidas para mejorar la postura de seguridad en el futuro.
	Monitoreo de Actividad de Acceso: Supervisar continuamente la actividad de acceso a los recursos en la nube para detectar posibles anomalías o comportamientos sospechosos. Utilizar herramientas de registro y monitoreo para capturar y analizar eventos de acceso, como intentos de inicio de sesión fallidos o cambios en los permisos. Realizar auditorías regulares de cumplimiento para asegurar que las políticas de IAM cumplan con los requisitos de seguridad y regulaciones aplicables.

Ilustración 1

Estructura Equipos y Roles – Modelo operativo Cloud Hibrido



El Diagrama ilustra una estructura organizacional propuesta para gestionar las operaciones en la nube en Anónima S.A., dividiendo las responsabilidades en tres equipos especializados: **Cloud Business Team**, **Cloud Platform Operation Team**, y **Cloud Platform Infrastructure**. Cada equipo está diseñado para abordar aspectos específicos de la operación, desde la alineación estratégica hasta la administración técnica de los recursos en la nube.

El modelo organizacional propuesto para Anónima S.A., basado en la integración de los equipos Cloud Business Team, Cloud Platform Operation Team y Cloud Platform Infrastructure, responde de manera estratégica a los desafíos actuales de la gestión en entornos híbridos y multicloud. La especialización de funciones permite abordar las necesidades de negocio, operación y soporte técnico de forma coordinada, eliminando los silos organizacionales tradicionales. Al incorporar mejores prácticas como ITIL, el Cloud Adoption Framework (CAF) y principios de DevSecOps, se garantiza una operación eficiente, escalable y segura, alineada con los objetivos estratégicos de la organización. Además, la división clara de responsabilidades fomenta la agilidad, reduce ineficiencias operativas y asegura un mejor uso de los recursos tecnológicos.

Ilustración 2

Estructura Equipos y Roles sin capacidades actuales en la organización – Modelo operativo Cloud Hibrido

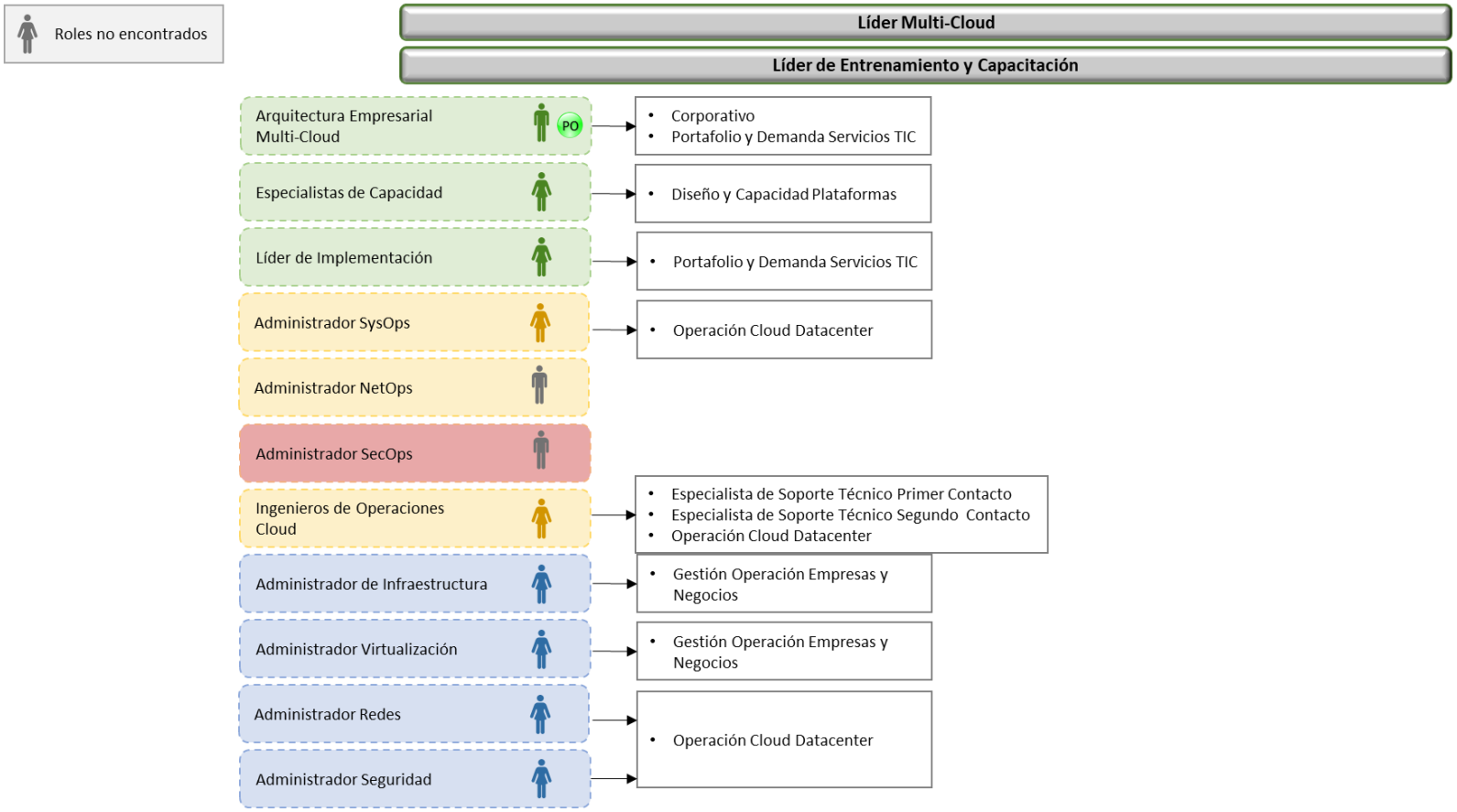


Ilustración 3

Distribución de transversal de roles por plataforma de Cloud – Modelo operativo Cloud Hibrido

La ilustración 2 compara los roles necesarios en el modelo operativo propuesto y la ilustración 3 plantea la distribución transversal de los roles e identifica las capacidades faltantes en la organización por plataforma de nube, para un entorno multicloud con los roles actualmente disponibles en la organización. Esta comparación resalta una diferencia importante entre las capacidades requeridas y las disponibles, evidenciada por los roles "no encontrados". Estas brechas incluyen posiciones críticas como el **Administrador NetOps Multi-Cloud**, el **Administrador SecOps Multi-Cloud**, y los roles relacionados con la gestión estratégica y operativa de entornos multicloud.

La conclusión principal es que la implementación exitosa del modelo operativo multicloud propuesto requerirá una transformación organizacional significativa, que debe incluir:

Desarrollo de Talento Interno: Capacitación intensiva para que el personal actual pueda adaptarse a los nuevos roles y responsabilidades, especialmente en áreas críticas como seguridad (SecOps), arquitectura empresarial y automatización.

Adquisición de Talento Especializado: Contratación de perfiles con experiencia en entornos multicloud, como arquitectos empresariales, especialistas en NetOps y SecOps, para llenar las vacantes detectadas.

Definición Clara de Roles y Responsabilidades: Establecer descripciones detalladas para cada uno de los nuevos roles propuestos, asegurando que se alineen con las necesidades estratégicas y operativas del modelo multicloud.

Promoción de la Colaboración Multidisciplinaria: Fomentar una integración más estrecha entre los equipos existentes y los nuevos roles, garantizando que el conocimiento del entorno actual se combine con las habilidades específicas para operar en la nube.

En resumen, el éxito de la propuesta dependerá de la capacidad de la organización para cerrar las brechas identificadas, fortaleciendo sus capacidades internas y asegurando que los roles críticos estén cubiertos. Esto no solo permitirá una adopción eficiente del modelo multicloud, sino que también

posicionará a la organización para aprovechar al máximo los beneficios de agilidad, eficiencia y escalabilidad que ofrece este entorno.

Recomendaciones para Anónima S.A.

Adopción de un modelo operativo basado en servicios:

Transformar el modelo operativo on-premises hacia un enfoque orientado a servicios, en el que los equipos gestionen productos o servicios específicos (por ejemplo, bases de datos como servicio o soluciones serverless), en lugar de gestionar únicamente infraestructura física.

Integrar prácticas de DevSecOps para fomentar la colaboración interdisciplinaria entre desarrollo, operaciones y seguridad.

Automatización de procesos:

Implementar herramientas como Terraform, Ansible o CloudFormation para manejar la infraestructura como código (Infrastructure as Code), eliminando tareas manuales repetitivas y reduciendo errores.

Automatizar el aprovisionamiento, la configuración y la gestión de recursos tanto en nubes públicas como on-premises.

Diseñar pipelines CI/CD para la automatización de despliegues, integrando seguridad desde las primeras etapas del desarrollo.

Capacitación continua y gestión del cambio organizacional:

Implementar un programa de capacitación en plataformas cloud (como AWS, Azure o Google Cloud), gobernanza de TI, herramientas de automatización y metodologías ágiles.

Realizar talleres para introducir conceptos como DevSecOps, IaC y estrategias de multicloud.

Gestionar el cambio organizacional mediante un plan que motive a los equipos a adoptar nuevas herramientas y procesos, minimizando la resistencia al cambio.

Implementación de un modelo híbrido y multicloud:

Diseñar un modelo de operación que integre servicios en nubes públicas y sistemas on-premises, aprovechando lo mejor de ambos mundos.

Evitar la dependencia de un solo proveedor de nube (vendor lock-in) mediante el uso de herramientas interoperables y estándares abiertos.

Utilizar estrategias de gobernanza multicloud para garantizar la consistencia en configuraciones y políticas de seguridad.

Optimización y gestión del consumo en la nube:

Establecer mecanismos de monitoreo y optimización de costos en la nube utilizando herramientas como AWS Cost Explorer, Azure Cost Management, o plataformas de terceros como CloudHealth.

Implementar políticas de etiquetado de recursos para rastrear el consumo por proyectos, equipos o departamentos.

Monitorear el uso de recursos para evitar sobredimensionamiento o subutilización, ajustando la capacidad según las demandas reales.

Fortalecimiento de la seguridad y la gobernanza:

Implementar un modelo de seguridad Zero Trust, garantizando el acceso basado en el principio de privilegio mínimo y autenticación multifactor (MFA).

Usar herramientas de gestión de identidades y accesos (IAM) para controlar quién puede acceder a qué recursos.

Establecer procesos para la protección de datos sensibles mediante cifrado y políticas de retención adecuadas.

Automatizar auditorías y cumplimiento normativo para reducir riesgos operativos y garantizar conformidad.

Planes de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DR):

Incluir características de BCP y DR desde el diseño de los servicios, como redundancia geográfica, respaldos automáticos y pruebas regulares de recuperación.

Diseñar escenarios de recuperación para diferentes niveles de incidentes, garantizando tiempos de recuperación (RTO) y puntos de recuperación de datos (RPO) alineados con los objetivos del negocio.

Realizar simulacros periódicos para validar la efectividad de los planes y preparar a los equipos.

Monitoreo centralizado y análisis de datos:

Implementar soluciones de monitoreo centralizado para correlacionar métricas de rendimiento y detectar anomalías en tiempo real.

Utilizar herramientas como Datadog, Prometheus o Elastic Stack (ELK) para la observabilidad y análisis en entornos híbridos y multicloud.

Integrar capacidades de análisis predictivo para anticipar posibles fallas o problemas operativos.

Reorganización de equipos hacia estructuras multidisciplinarias:

Reconfigurar los equipos tradicionales (servidores, almacenamiento, redes) en equipos orientados a productos o servicios, capaces de abarcar múltiples áreas tecnológicas.

Crear roles híbridos como Cloud Engineers, Site Reliability Engineers (SREs) y Cloud Architects que puedan gestionar y optimizar recursos tanto en la nube como on-premises.

Fomentar la comunicación y colaboración entre equipos para romper los silos organizacionales.

Medición y mejora continua del modelo operativo:

Definir métricas clave (KPIs) para medir la eficiencia, costos, y satisfacción del usuario final en los servicios gestionados.

Revisar periódicamente el modelo operativo para identificar áreas de mejora y adaptarse a cambios tecnológicos o del mercado.

Incorporar herramientas analíticas transversales para identificar patrones de uso, optimizar recursos y proponer mejoras.

Conclusiones

Las limitaciones identificadas en el modelo actual de TI de Anónima S.A., como la operación en silos y la dependencia de recursos locales, generan ineficiencias operativas, costos elevados y dificultades en la integración con la nube. La transición a un modelo híbrido requiere superar estos desafíos mediante la automatización, la capacitación del personal y la adopción de estructuras organizacionales más flexibles que permitan la interoperabilidad y optimización de recursos.

Los marcos de trabajo, como el Cloud Adoption Framework (CAF) e ITIL, ofrecen directrices fundamentales para estructurar la adopción de un modelo operativo híbrido en Anónima S.A. Estos enfoques permiten establecer una estrategia clara para la gestión de recursos en la nube, alineando la operación tecnológica con los objetivos de negocio y asegurando la optimización de costos, la seguridad y la eficiencia operativa. Su aplicación facilita la interoperabilidad entre entornos on-premises y en la nube, minimizando riesgos y mejorando la gobernanza de TI.

Además, la adopción de estos marcos fomenta la estandarización de procesos y la automatización, lo que reduce la dependencia de estructuras organizacionales tradicionales en silos. La implementación de ITIL garantiza una gestión eficiente de servicios y soporte, mientras que el CAF proporciona una metodología integral para la adopción y madurez del modelo híbrido. En conjunto, estos enfoques fortalecen la capacidad de adaptación de la organización ante cambios tecnológicos y contribuyen a una transformación digital sostenible.

La propuesta para Anónima S.A. integra sus capacidades actuales, combinando el conocimiento del recurso humano y la operación on-premises con un modelo híbrido que optimiza la gestión de TI y facilita la adopción de la nube. Este enfoque permitirá una transición gradual sin afectar la continuidad operativa, maximizando el uso de la infraestructura existente y minimizando costos. Además, la

implementación de marcos de gobernanza como ITIL y el Cloud Adoption Framework (CAF) asegura una gestión eficiente de los recursos, mientras que la capacitación del equipo fortalece su adaptación a nuevas tecnologías. Con ello, Anónima S.A. moderniza su infraestructura tecnológica sin perder el control operativo, potenciando su capacidad de respuesta y sostenibilidad en un entorno digital en constante evolución.

Referencias

Tornatzky, L. G., & Fleischer, M. (1990). The Processes of Technological Innovation. Lexington Books.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. Recuperado de https://csrc.nist.gov/publications/detail/sp/800-145/final

AXELOS. (2019). ITIL Foundation, ITIL 4 Edition. Stationery Office.

Microsoft. (2023). Azure Cloud Adoption Framework Handbook. Recuperado de https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/

Chang, V. (2020). A proposed framework for cloud computing adoption. International Journal of Organizational and Collective Intelligence, 6(3), 1–12. https://doi.org/10.4018/978-1-5225-9615-8.ch044

Qatawneh, N. (2024). Building a framework to drive government systems' adoption of cloud computing. Discover Sustainability. https://doi.org/10.1007/s43621-024-00013-2

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2022). Metodología de la investigación (7ª ed.). McGraw-Hill Education.

National Institute of Standards and Technology (NIST). (2011). The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology. Special Publication 800-145. Recuperado de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Amazon Web Services. (2024). AWS Cloud Adoption Framework. Recuperado de https://aws.amazon.com/caf/

Kovacevic, S., & Dempsey, D. (2023). Azure Cloud Adoption Framework Handbook. Birmingham-Mumbai: Packt Publishing.

Alqatan, S., Alshirah, M., & Bany Baker, M. (2025). A conceptual framework for cloud computing adoption in higher education institutions. Data and Metadata, 4(431). https://doi.org/10.56294/dm2025431

Saratchandra, P., & Shrestha, B. (2022). Multicloud adoption in hybrid IT environments: A governance perspective. International Journal of Cloud Computing, 10(1), 25–37. https://doi.org/10.1504/IJCC.2022.10045698

Fernández, A., Peralta, D., Herrera, F., & Benítez, J. M. (2014). An overview of the role of cloud computing in higher education. IEEE Transactions on Education, 57(2), 88–95. https://doi.org/10.1109/TE.2013.2284155

Carayannis, E. G., Grigoroudis, E., Stamati, T., & Valvi, T. (2021). Digital transformation and business model innovation: A conceptual framework. Journal of Business Research, 123, 291–300. https://doi.org/10.1016/j.jbusres.2020.09.037