# IMPLEMENTACIÓN WELL-ARCHITECTED FRAMEWORK EN ENTORNOS MULTI-SUSCRIPCIÓN

HAROL CAMILO PINTO GOMEZ – JULIAN ANDREY PUERTO CORRAL

Directores:
MARTHA ISABEL VILLARREAL LOPEZ

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN GESTIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN
BOGOTÁ, 2026

# Tabla de Contenido

## ACRÓNIMOS

- IMSM – Implementación Multi-Suscripción en Microsoft
- WAF-MS – Well-Architected Framework Multi-Subscription
- GEMC – Gobernanza en Entornos Multi-Cloud
- GEMS – Gobernanza de Entornos Multi-Suscripción
- MAOM – Modelo de Arquitectura Operativa Multi-suscripción
- AEGC – Arquitectura Empresarial Gobernada en Cloud
- MOGC – Modelo Operativo de Gobernanza Cloud
- EMAC – Estrategia Multi-suscripción en Azure Corporativo

- Excelencia Operacional
    - EOA – Excelencia Operacional en Azure
    - AOM – Automatización Operativa Multi-suscripción

- • Seguridad
    - SEG-MSA – Seguridad en Multi-Suscripción Azure
    - IAM-C – Identity & Access Management Corporativo

- Fiabilidad
    - RCA – Resiliencia Cloud en Azure
    - FMS – Fiabilidad Multi-Suscripción
-
- Eficiencia de rendimiento
    - ERP-AZ – Eficiencia de Rendimiento en Azure
    - OPR – Optimización de Performance de Recursos

- Optimización de costos
    - COC – Control y Optimización de Costos
    - FCO – FinOps Cloud Operativo

## RESUMEN

El presente documento aborda la implementación del Azure Well-Architected Framework (WAF) de Microsoft en un tenant corporativo que administra más de cinco suscripciones activas en Azure, cada una con cargas de trabajo, equipos y requisitos de cumplimiento diferenciados. El problema central identificado es la gestión ineficiente y desorganizada del entorno multi-suscripción, provocada por la ausencia de un modelo de gobernanza, la falta de segmentación de redes, el aprovisionamiento no estandarizado de recursos y el desconocimiento de buenas prácticas en arquitectura cloud por parte de los administradores.

Con base en los cinco pilares del WAF — Excelencia Operacional, Seguridad, Fiabilidad, Eficiencia de Rendimiento y Optimización de Costos — el trabajo propone un enfoque sistemático para diagnosticar las brechas existentes, diseñar lineamientos de gobernanza, estandarizar políticas mediante herramientas como Azure Policy, Management Groups y RBAC, y definir una arquitectura objetivo que garantice la segmentación de ambientes, la estandarización de nomenclaturas y entornos homogéneos. El resultado esperado es un modelo de gobernanza cloud escalable y seguro que alinee las decisiones técnicas con los objetivos estratégicos de la organización, reduzca riesgos operativos y financieros, y promueva una cultura de arquitectura responsable.



**Palabras clave:** Azure Well-Architected Framework, gobernanza cloud, multi-suscripción, Microsoft Azure, seguridad, excelencia operacional, optimización de costos.

## ABSTRACT

This paper presents the implementation of the Microsoft Azure Well-Architected Framework (WAF) in a corporate tenant managing more than five active Azure subscriptions, each with distinct workloads, responsible teams, and compliance requirements. The central problem identified is the inefficient and disorganized management of the multi-subscription environment, caused by the absence of a governance model, lack of network segmentation, non-standardized resource provisioning, and limited knowledge of cloud architecture best practices among subscription administrators.

Based on the five pillars of the WAF — Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization — this work proposes a structured approach to diagnose existing gaps, design governance guidelines, standardize policies using tools such as Azure Policy, Management Groups, and RBAC, and define a target architecture that ensures environment segmentation, resource naming standards, and homogeneous environments. The expected outcome is a scalable and secure cloud governance model that aligns technical decisions with the organization's strategic objectives, reduces operational and financial risks, and fosters a culture of responsible architecture.



Keywords: Azure Well-Architected Framework, cloud governance, multi-subscription, Microsoft Azure, security, operational excellence, cost optimization.

# INTRODUCCIÓN

El entorno empresarial se caracteriza por una complejidad y dinamismo creciente, y la adopción de arquitecturas cloud debe ser ya no sólo eficiente en su operativa, sino que también debe establecer un enfoque estructural que garantice la seguridad, la fiabilidad y la escalabilidad de las soluciones desplegadas a través de dichas arquitecturas. Microsoft Azure es una de las plataformas de servicios en la nube, que ha desarrollado el Well-Architected Framework (WAF), el cual establece unas buenas prácticas para que las organizaciones puedan diseñar, construir y, en su caso, mantener cargas de trabajo en la nube alineadas con unos sólidos principios arquitectónicos. Este documento discute la implementación del Azure Well-Architected Framework en un tenant corporativo que gestiona más de cinco suscripciones activas, cada una de estas suscripciones cuenta con distintas cargas de trabajo, equipos responsables y diferentes requerimientos de cumplimiento.

Esta implementación tiene como propósito establecer un modelo de enfoque estandarizado, con el objetivo de mejorar la gobernanza, la eficiencia operativa, la seguridad y la sostenibilidad del entorno cloud, de forma que queden mitigados los riesgos comunes a configuraciones desalineadas o al crecimiento descontrolado.
El objetivo del paper es detallar los desafíos, estrategias y resultados obtenidos al aplicar los cinco pilares del Azure Well-Architected Framework —Excelencia Operacional, Seguridad, Fiabilidad, Eficiencia de Rendimiento y Optimización de Costos— en un contexto multi-suscripción, sirviendo como referencia práctica para otras organizaciones con necesidades similares.

Ampliando la variedad de suscripciones o de equipos, o incluso de objetivos en el tenant; la adopción del Well-Architected Framework no es sólo una forma de conseguir una mejora tanto de la postura técnica como la operativa del cliente sino también el lugar donde se puede sentar y empezar a implantar una cultura en pro de una arquitectura responsable. Las bases comunes, unos modelos de gobernanza claros y la visibilidad del entorno transversalmente habilitan un modelo de gestión ágil, seguro y sostenible que permite alinear las decisiones técnicas con los objetivos estratégicos del cliente, disminuir riesgos y optimizar la inversión en la nube.

## PROBLEMA

El problema planteado para esta investigación es la Gestión ineficiente y desorganizada del entorno multi-suscripción en Azure debido a la ausencia de gobernanza y buenas prácticas.

## ÁRBOL DE PROBLEMAS

El siguiente diagrama representa un árbol de problemas cuyo nodo central identifica la causa raíz del sistema analizado: la gestión ineficiente y desorganizada del entorno multi-suscripción en Azure, originada por la ausencia de gobernanza y buenas prácticas. A partir de este núcleo se desprenden tres causas estructurales interrelacionadas:

1. Falta de gobernanza en la nube - derivada de la inexistencia de políticas centralizadas de acceso, seguridad y control de costos, lo que produce recursos mal dimensionados, sin seguimiento de uso y con dificultades para la optimización del gasto.
2. Proliferación descontrolada de suscripciones y recursos - generada por la creación de recursos sin estandarización y la duplicación de esfuerzos, lo que imposibilita la auditoría del entorno y dificulta la escalabilidad ordenada de soluciones.
3. Desconocimiento de buenas prácticas por parte de los propietarios - evidenciado en la escasa formación técnica en arquitectura cloud y la administración autónoma sin coordinación, lo que resulta en decisiones técnicas desalineadas con la estrategia organizacional y pérdida de eficiencia en proyectos críticos.
4. Como efecto transversal, estas tres causas convergen en una ausencia de segmentación de redes y seguridad, donde los entornos de prueba y producción coexisten sin aislamiento lógico, no se aplican controles como NSGs (Network Security Groups), firewalls o subredes adecuadas, exponiendo el sistema a vulnerabilidades y potenciales brechas de datos.

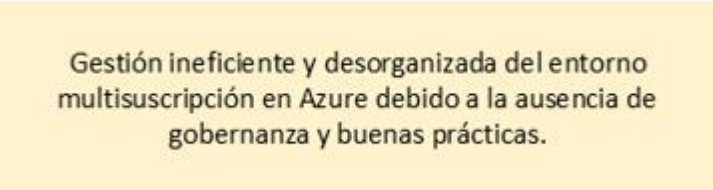


Ilustración 1 Árbol de Problemas – Problema Principal

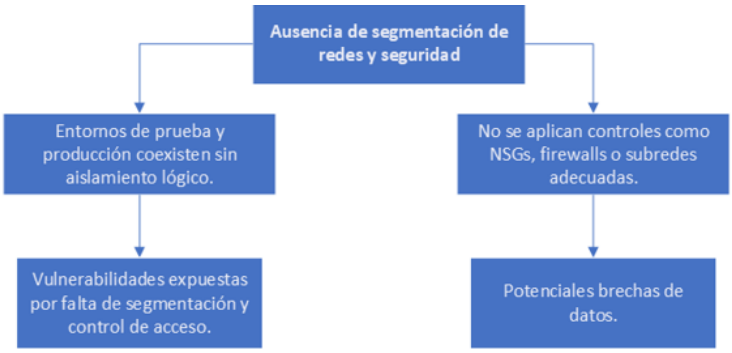


Ilustración 2 Árbol de Problemas – Problema Secundario 1

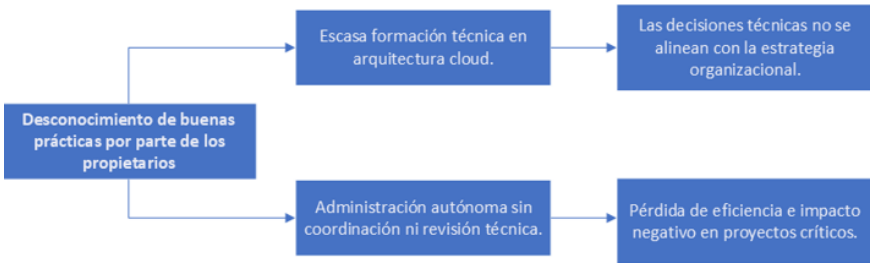


Ilustración 3 Árbol de Problemas – Problema Secundario 2

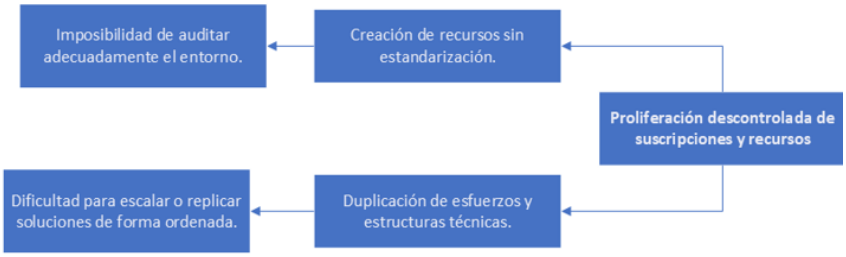


Ilustración 4 Árbol de Problemas – Problema Secundario 3

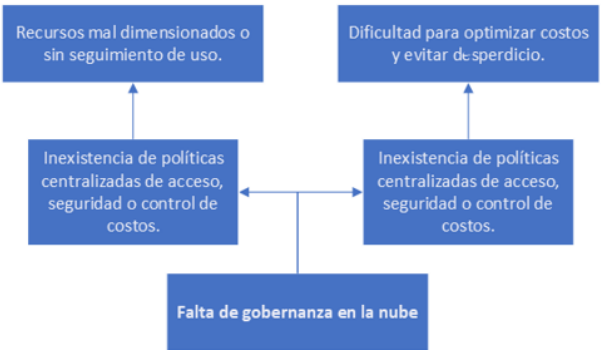


Ilustración 5 Árbol de Problemas – Problema Secundario 4

## ¿QUÉ SE QUIERE SOLUCIONAR?

El acelerado auge del uso de servicios en la nube en muchas organizaciones ha derivado, en la mayoría de los casos, en la improvisada creación de suscripciones, entornos y recursos en el uso de plataformas como Microsoft Azure. En el caso concreto de este trabajo, podemos observar un tenant corporativo que gestiona más de cinco suscripciones y cuya gestión se hace sin definir un modelo de gobernanza, lo que resulta en la fragmentación del entorno, carente de lineamientos compartidos, controles de seguridad estandarizados y mecanismos de operación óptimos para la operación de la entidad. Se observan los siguientes ítems para tener en cuenta para resolución:

- Ausencia de gobernanza sobre componentes asociados a diversas suscripciones (Etiquetado, nombramiento, gestión de costos, aplicación y cumplimiento de directivas y políticas personalizadas y nativas - creación de segmentos de red y permisos asignadas a cada segmento (gobernanza en networking).
- Documentación desactualizada o inexistente sobre el aprovisionamiento de componente y/o aplicaciones
- Sin segmentación de ambientes.
- Aprovisionamiento de componentes en nube sin estandarización o política de nombramiento (tags).
- Ausencia de diagramas de arquitectura de aplicaciones aprovisionadas.
- Ausencia de redundancias de aplicación como componente de infraestructura tecnológica.

  En los siguientes diagramas de arquitectura producto del diagnóstico realizado por el equipo de trabajo, observamos una ausencia de segmentación adecuada de los recursos en diferentes entornos de soluciones con múltiples propósitos, agrupados en grupos de recursos, pero sin una separación lógica de red o de seguridad o por componente.

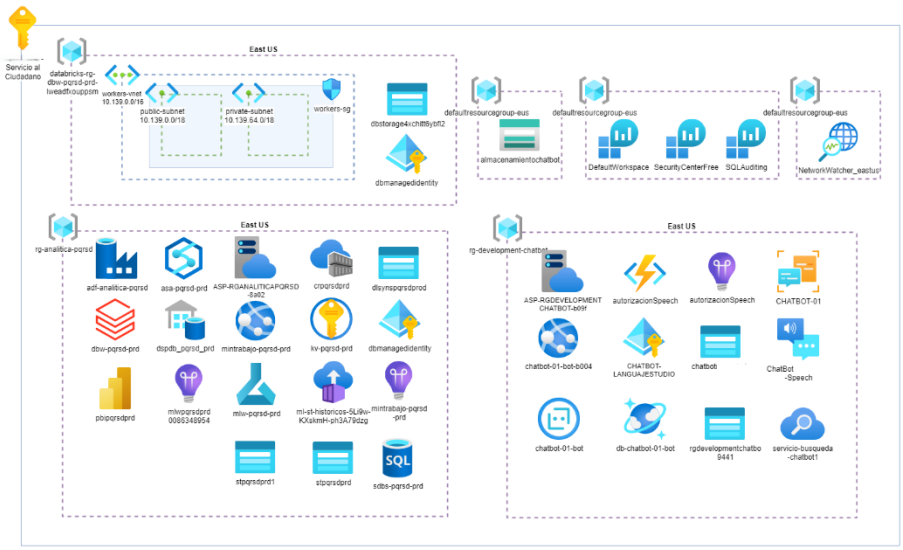


Ilustración 6 Suscripción ejemplo sin WAF aplicado

A continuación, observamos que existen múltiples suscripciones con diferentes segmentos de red que genera overlap en la conexión entre suscripciones, sin un orden lógico o tablas de enrutamiento que permitan una asignación de direccionamiento más ordenado y sin interrupciones de conexión entre las mismas.

Ilustración 7 Segmentación

## IDEACIÓN DE LA SOLUCIÓN

La presente investigación está centrada en aplicar el Azure Well-Architected Framework (WAF) en un tenant corporativo en el que existen más de cinco suscripciones activas en Microsoft Azure. El alcance del trabajo comprende tanto el diagnóstico del estado actual del entorno, así como la detección de brechas con respecto a las mejores prácticas del WAF, así como la definición e implementación de acciones correctivas, alineadas con los cinco pilares del WAF: Excelencia Operacional, Seguridad, Fiabilidad, Eficiencia de Rendimiento y Optimización de Costos.

## ¿POR QUÉ SE PLANTEA AHORA LA SOLUCIÓN?

La falta de recomendaciones de uso ha hecho proliferar entornos de prueba y de producción que coexisten de manera no separada a nivel de red, incrementando enormemente la superficie de ataque y de fuga de datos. Además, no se han implementado políticas de acceso, control del coste y auditoría de recursos, lo que lleva a incrementar los riesgos operativos y los riesgos financieros. Los riesgos se ven además incrementados por el conocimiento escaso de las mejores prácticas en arquitectura de la nube por parte de los administradores de las suscripciones, que muchas veces gestionan sin coordinación y visibilidad.
La falta de un marco de referencia estandarizado para poder garantizar la disponibilidad, escalabilidad y seguridad a nivel de soluciones implementadas en Azure, así como mantener un marco de referencia para la operación con las soluciones que permitan auditar y detectar las vulnerabilidades existentes, hace más complicado la administración de estos entornos.

Este contexto evidencia la necesidad urgente de adoptar un enfoque sistemático, como el proporcionado por el Azure Well-Architected Framework, que permita establecer una base sólida para la operación y evolución del entorno de nube corporativo.

## SECTOR OBJETIVO

El sector objetivo de la presente propuesta corresponde a organizaciones del sector público que han iniciado procesos de adopción de servicios en nube pública, particularmente sobre Microsoft Azure, pero que no cuentan con una estructura de arquitectura, gobernanza, operación y control previamente definida. Este tipo de organizaciones suele migrar o desplegar soluciones en la nube como respuesta a

necesidades inmediatas de disponibilidad, escalabilidad, continuidad operativa o modernización tecnológica, pero sin haber establecido previamente lineamientos formales para la administración del entorno cloud.

Dentro de este sector se encuentran entidades públicas, instituciones educativas, empresas prestadoras de servicios, organizaciones del sector salud, entidades financieras entre otras organizaciones que han incorporado Azure como plataforma de operación, pero cuya adopción se ha realizado de manera progresiva, reactiva o descentralizada. En estos contextos, es común encontrar múltiples suscripciones activas, recursos desplegados por diferentes equipos, ambientes de pruebas y producción mezclados, nomenclaturas inconsistentes, ausencia de documentación técnica y controles de seguridad aplicados de manera parcial.

El sector público representa un campo especialmente relevante para esta propuesta, debido a que muchas entidades estatales adelantan procesos de transformación digital orientados a mejorar la prestación de servicios, fortalecer la relación con los ciudadanos y aumentar la eficiencia institucional. En Colombia, la Política de Gobierno Digital busca precisamente fortalecer la transformación digital pública, mejorar la prestación de servicios y generar confianza institucional mediante el uso y aprovechamiento de las TIC ( Ministerio de Tecnologías de la Información de Colombia, 2026). Sin embargo, la adopción de nube pública en este tipo de organizaciones puede enfrentar limitaciones asociadas a obsolescencia tecnológica, restricciones presupuestales, baja madurez digital, falta de perfiles especializados y ausencia de modelos claros de gobierno tecnológico.

El tipo de cliente objetivo se caracteriza por tener una infraestructura tecnológica previa con señales de obsolescencia, aplicaciones heredadas, procesos manuales, documentación incompleta, baja estandarización operativa y equipos técnicos con conocimiento limitado sobre servicios cloud. Estas organizaciones pueden haber desplegado máquinas virtuales, bases de datos, redes virtuales, cuentas de almacenamiento, servicios PaaS o componentes de seguridad en Azure, pero sin una comprensión integral de cómo estos recursos deben organizarse dentro de una arquitectura escalable, segura y gobernada.

La propuesta se enfoca especialmente en organizaciones que tienen múltiples áreas internas, proveedores o equipos técnicos administrando recursos de nube de forma independiente. Esta condición genera una pérdida de visibilidad transversal, duplicidad de recursos, incremento de costos, exposición a riesgos de seguridad y dificultad para aplicar políticas comunes. En estos escenarios, la ausencia de

Management Groups, Azure Policy, RBAC (Role Based Access Control) o controles de acceso basados en roles, estándares de etiquetado, segmentación de red y modelos de monitoreo centralizado limita la capacidad de control de la organización.

Las aplicaciones del sector incluyen soluciones misionales, portales web, sistemas de información internos, aplicaciones de gestión documental, plataformas analíticas, servicios de integración, ambientes de desarrollo, soluciones de atención ciudadana, sistemas transaccionales, repositorios de datos y servicios de automatización. Estas soluciones pueden operar sobre infraestructura como servicio, plataforma como servicio o arquitecturas híbridas, pero requieren un marco de control común que permita administrarlas de manera segura, eficiente y alineada con los objetivos institucionales.

La relación de estas aplicaciones con la propuesta es directa, ya que el Azure Well-Architected Framework (Microsoft, 2026) permite evaluar, ordenar y mejorar las cargas de trabajo existentes en función de cinco pilares: confiabilidad, seguridad, optimización de costos, excelencia operacional y eficiencia de rendimiento. Microsoft define este framework como un conjunto de principios, decisiones arquitectónicas y herramientas de revisión orientadas a construir una base técnica sólida para las cargas de trabajo en Azure. Por tanto, el sector objetivo no se limita a organizaciones que apenas van a iniciar su camino hacia la nube, sino principalmente a aquellas que ya han implementado soluciones cloud sin una arquitectura suficientemente madura y necesitan reorganizar, gobernar y optimizar su entorno.

## TENDENCIAS DEL SECTOR

Las organizaciones públicas se encuentran en un proceso creciente de transformación digital, impulsado por la necesidad de modernizar sus servicios, mejorar la eficiencia operativa, optimizar costos y responder con mayor agilidad a las demandas de usuarios, ciudadanos, clientes y áreas internas. En este contexto, la nube pública se ha convertido en un habilitador tecnológico clave, al permitir el acceso bajo demanda a servicios de cómputo, almacenamiento, bases de datos, redes, analítica, inteligencia artificial, seguridad y automatización. Microsoft Azure define la computación en la nube como la entrega de servicios de cómputo a través de internet, incluyendo servidores, almacenamiento, bases de datos, redes, software, analítica e inteligencia (Microsoft, 2026).

Una tendencia marcada claramente es la consolidación de modelos de gobernanza cloud. A medida que las organizaciones aumentan el número de suscripciones, recursos, usuarios y cargas de trabajo en Azure, se vuelve indispensable definir estructuras de administración centralizada. El Cloud Adoption Framework (Microsoft, 2023) de Microsoft recomienda el uso de Management Groups para agregar asignaciones de políticas e iniciativas mediante Azure Policy, así como la aplicación de RBAC para controlar la autorización sobre las operaciones de administración (Microsoft, 2025). Esta tendencia responde a la necesidad de pasar de una adopción cloud informal a un modelo operativo controlado, auditable y sostenible. En el sector público, la transformación digital también se relaciona con la generación de valor público, interoperabilidad, seguridad de la información y mejora de la experiencia ciudadana. La Estrategia Nacional Digital de Colombia 2023-2026 plantea una visión sobre el acceso, uso y apropiación de datos y tecnologías digitales como parte de los esfuerzos de transformación digital del país (Ministerio de Tecnologias de la Información de Colombia, 2023). Esto refuerza la necesidad de que las entidades no solo adopten tecnología, sino que lo hagan bajo modelos sostenibles, seguros y gobernados.

Finalmente, se observa una tendencia hacia la alfabetización cloud de equipos técnicos y directivos. La implementación de nube pública no puede depender únicamente de la capacidad de desplegar recursos, sino de comprender los modelos de responsabilidad compartida, los tipos de servicio, los riesgos de configuración, los costos asociados, la seguridad por diseño y las implicaciones de arquitectura. Por ello, la aplicación de frameworks como Azure Well-Architected Framework y Cloud Adoption Framework se vuelve una práctica necesaria para reducir la brecha entre adopción tecnológica y madurez operativa.

## ANÁLISIS DE MERCADO

El mercado objetivo de la presente propuesta está conformado por entidades del sector público que han iniciado procesos de adopción de nube pública, particularmente sobre Microsoft Azure, pero que no cuentan con una arquitectura previamente definida ni con un modelo formal de gobernanza, operación, seguridad y control de costos. Este tipo de entidades suele adoptar servicios cloud para responder a necesidades institucionales como continuidad operativa, modernización tecnológica, disponibilidad de servicios digitales, reducción de infraestructura física, interoperabilidad, analítica de datos o fortalecimiento de canales de atención ciudadana. En Colombia, la transformación digital pública se ha convertido en un eje estratégico para mejorar la relación entre el Estado y los

ciudadanos. La Política de Gobierno Digital busca fortalecer la prestación de servicios, generar confianza institucional y promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones en las entidades públicas. Esta política hace parte del Modelo Integrado de Planeación y Gestión —MIPG— y aplica a las entidades de la administración pública y a particulares que cumplen funciones administrativas. ( Ministerio de Tecnologías de la Información de Colombia, 2026). Dentro de este contexto, existe una necesidad creciente de servicios especializados que permitan a las entidades públicas pasar de una adopción tecnológica reactiva a un modelo de operación digital estructurado. Muchas entidades han implementado soluciones en la nube mediante proyectos independientes, contratos específicos o necesidades urgentes de operación, pero sin una visión integral sobre arquitectura empresarial, seguridad, gestión de identidades, segmentación de red, monitoreo, continuidad, costos y documentación técnica. Esta situación genera una oportunidad de mercado para servicios de consultoría orientados al diagnóstico, reorganización y maduración de entornos cloud.

Desde el punto de vista de la oferta, el mercado cuenta con proveedores de servicios cloud, integradores tecnológicos, fabricantes, partners de Microsoft, firmas de consultoría y contratistas especializados que ofrecen servicios de migración, soporte, administración, licenciamiento o implementación de recursos en la nube. Sin embargo, no todas las ofertas se enfocan en el diagnóstico de madurez arquitectónica ni en la corrección de entornos cloud ya implementados sin gobierno. En este punto se identifica una oportunidad diferencial: prestar un servicio que no solo despliegue tecnología, sino que evalúe el estado actual, identifique brechas, proponga una arquitectura objetivo y defina una hoja de ruta de mejora alineada con buenas prácticas.

El mercado público también cuenta con mecanismos de compra tecnológica que facilitan la adquisición de servicios cloud. Colombia Compra Eficiente dispone del Acuerdo Marco de Precios de Servicios de Nube Pública V, vigente desde el 5 de marzo de 2026 hasta el 5 de marzo de 2028, cuyo objeto incluye seleccionar proveedores de servicios de nube pública y definir condiciones para que las entidades estatales contraten estos servicios. Este acuerdo contempla segmentos de proveedores como Microsoft y permite contratar servicios asociados a nube pública bajo condiciones predefinidas para las entidades estatales. (Agencia Nacional de Contratación Pública CCE, 2026). No obstante, aunque el Acuerdo Marco permite adquirir servicios cloud, las entidades siguen necesitando capacidades internas o acompañamiento especializado para tomar decisiones

correctas sobre arquitectura, gobierno y operación. La existencia de un mecanismo de compra no garantiza por sí sola que los recursos contratados se implementen con buenas prácticas. Por esta razón, el servicio propuesto se posiciona como una consultoría de valor agregado que puede complementar la adquisición de nube pública mediante diagnóstico, diseño de arquitectura, definición de políticas, priorización de riesgos y transferencia de conocimiento. La oportunidad de mercado también se fortalece por la actualización de lineamientos de seguridad digital en el país. El Modelo de Seguridad y Privacidad de la Información —MSPI— orienta a las entidades públicas en la adopción de buenas prácticas para gestionar el ciclo de vida de la seguridad de la información, incluyendo planeación, implementación, evaluación y mejora continua. El MSPI busca incorporar la seguridad de la información en procesos, trámites, servicios, sistemas de información, infraestructura y activos de información, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos. (Ministerio de Tecnológias de la Información, 2025).

Desde una perspectiva competitiva, la propuesta se diferencia porque integra tres dimensiones que muchas veces se abordan por separado: arquitectura cloud, gobernanza institucional y madurez operativa. No se limita a recomendar recursos de Azure ni a ejecutar configuraciones aisladas, sino que plantea una intervención consultiva que parte del diagnóstico, identifica brechas frente al WAF, define una arquitectura objetivo, propone políticas de gobernanza y acompaña a la entidad en una adopción progresiva, medible y sostenible.

## OBJETIVO

Implementar el Azure Well-Architected Framework en un tenant con múltiples suscripciones activas, con el fin de establecer un modelo de gobernanza y operación que mejore la eficiencia, seguridad, confiabilidad y optimización de recursos en el entorno de nube corporativo.

## OBJETIVOS ESPECÍFICOS

- Diagnosticar el estado actual de las suscripciones existentes, identificando brechas y desviaciones respecto a las prácticas recomendadas por el Azure Well-Architected Framework.

- Diseñar lineamientos y mecanismos de gobernanza basados en los cinco pilares del framework, aplicables de manera consistente en todas las suscripciones del tenant.
- Implementar una política de Gobernanza de Nube Pública que permita a la organización tener un estándar de gestión y administración transversal a proveedores y operadores internos y externos.
- Evaluar el impacto de la implementación del framework mediante métricas clave, con foco en la mejora continua de operaciones, seguridad y costos a nivel organizacional.

## ÁRBOL DE OBJETIVOS

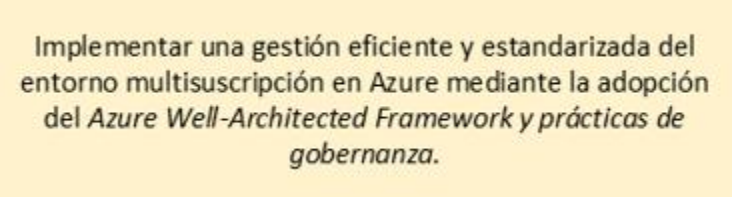


Ilustración 8 Árbol de Objetivos – Objetivo Principal

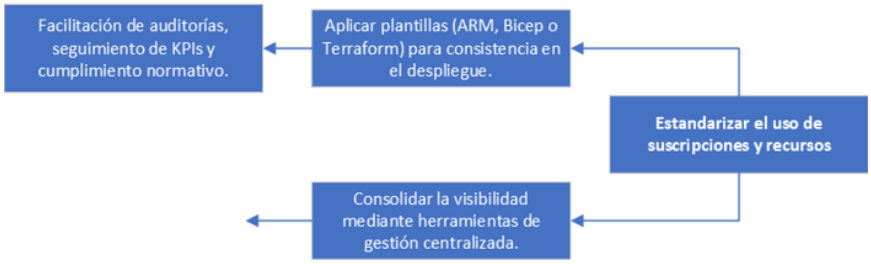


Ilustración 9 Árbol de Objetivos – Objetivos Secundarios 1


Ilustración 10 Árbol de Objetivos – Objetivos Secundarios 2

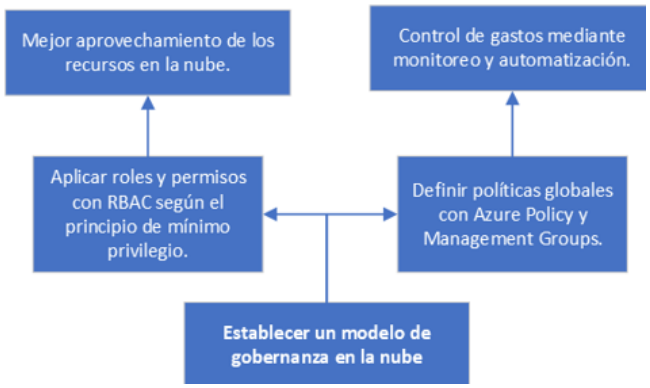


Ilustración 11 Árbol de Objetivos – Objetivos Secundarios 3

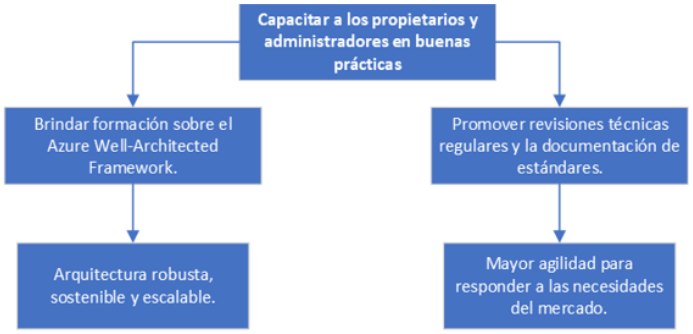


Ilustración 12 Árbol de Objetivos – Objetivos Secundarios 4

El anterior diagrama representa un árbol de objetivos cuyo nodo central define la meta general del proyecto: implementar una gestión eficiente y estandarizada del entorno multi-suscripción en Azure, mediante la adopción del Azure Well-Architected Framework y prácticas de gobernanza. A partir de este objetivo central se desprenden cuatro líneas de acción estratégicas:

1. Establecer un modelo de gobernanza en la nube - mediante la definición de políticas globales con Azure Policy y Management Groups, y la aplicación de roles y permisos bajo el principio de mínimo privilegio con RBAC (Role Based Access). Esto permite un mejor aprovechamiento de los recursos y el control de gastos mediante monitoreo y automatización.
2. Estandarizar el uso de suscripciones y recursos - a través de la aplicación de plantillas de infraestructura como código IaC (Terraform) para garantizar consistencia en el despliegue, y la consolidación de visibilidad mediante herramientas de gestión centralizada. Como resultado se facilitan auditorías, el seguimiento de KPIs y el cumplimiento normativo.
3. Diseñar y aplicar una segmentación adecuada de redes y seguridad - separando los entornos de desarrollo, pruebas y producción mediante

subredes y NSGs (Network Security Groups), e implementando controles de seguridad como firewalls, monitorización y alertas. Esto se traduce en mayor protección de datos y activos críticos, y en la disminución de configuraciones vulnerables.

4. Capacitar a los propietarios y administradores en buenas prácticas - mediante formación en el Azure Well-Architected Framework y la promoción de revisiones técnicas regulares con documentación de estándares, logrando una arquitectura robusta, sostenible, escalable y con mayor agilidad de respuesta ante las necesidades del negocio.

## ¿CUÁL ES LA SITUACIÓN DESEADA?

La computación en la nube ha modificado por completo los métodos que utilizan las organizaciones para crear, implantar y escalar sus soluciones tecnológicas. Plataformas como Microsoft Azure ofrecen servicios bajo demanda y permiten realizar una adopción de modelos de infraestructura menos rígidos, además de experimentar un paso considerablemente menor para la implementación y un mejor control de los costes. No obstante, a medida que las organizaciones van escalando sus operaciones en la nube, también van surgiendo nuevos retos de gobernanza, seguridad, cumplimiento normativo y administración de recursos distribuidos.

En contextos con múltiples suscripciones resulta frecuente que diferentes unidades de negocio, departamentos o equipos de desarrollo gestionen únicamente sus propios recursos. Esto puede dificultar la posibilidad de una visibilidad centralizada, provocar duplicaciones de esfuerzo y generar vulnerabilidades de seguridad o bien llevar a un uso más ineficiente de los recursos. Por ello, es necesario un enfoque sistemático que alinee todas las suscripciones entorno a principios arquitectónicos comunes y operativos que aseguren una operación coherente, segura y eficiente.

## INTRODUCCIÓN A LA SITUACIÓN DESEADA

El Azure Well-Architected Framework es una guía que proporciona Microsoft y es una colección de principios para el diseño y la operación de cargas de trabajo mejor concebido en Azure. Es un framework con cinco pilares:

- Excelencia Operacional: ya que se centra en las operaciones eficaces, la automatización, la supervisión continua y la capacidad de respuesta ante eventos operativos.

- Seguridad: que consiste en la protección de los datos, la gestión de la identidad, el establecimiento de controles de acceso, la defensa ante amenazas internas y externas.
- Fiabilidad: que es asegurar que los sistemas puedan recuperarse de un error y escalar según demanda, sin ningún fallo que cause interrupciones.
- Eficiencia de Rendimiento: que se basa en el uso óptimo de los recursos informáticos existentes, ajustando cargas de trabajo para conseguir el mejor rendimiento.
- Optimización de Costos: que se refiere a un uso eficiente de los recursos, evitando gastos innecesarios para así mejorar el retorno de la inversión.

La implementación del WAF permite a las organizaciones auditar sus cargas de trabajo mediante revisiones sistemáticas (Well-Architected Reviews), detectar áreas de mejora y establecer prioridades de las acciones a llevar a cabo, basado en las buenas prácticas reconocidas por la industria basados en modelos de gobernanza. La gobernanza de Azure hace referencia a todas aquellas políticas, procesos y estructuras que permiten gestionar el uso de la plataforma de forma segura y eficiente. Para tenants con varias suscripciones, las herramientas Azure Policy, Azure Blueprints, Management Groups y Azure Lighthouse son clave para aplicar normas globales, delegar responsabilidades o automatizar el cumplimiento.
Una buena adopción del Well-Architected Framework tiene que ir de la mano de un modelo de gobernanza que permita aplicar las recomendaciones del WAF de manera transversal sobre todas las suscripciones, sin perder flexibilidad para casos concretos.

## PROPUESTA DE VALOR

Ofrecer a organizaciones públicas un modelo estructurado para diagnosticar, organizar, gobernar y optimizar entornos de Microsoft Azure que han sido implementados sin una arquitectura previamente definida. La solución está orientada a organizaciones que ya tienen recursos desplegados en la nube, pero que presentan brechas de gobernanza, seguridad, documentación, segmentación, nomenclatura, control de costos y operación centralizada.

El valor principal de la propuesta radica en traducir buenas prácticas y frameworks de arquitectura cloud en acciones concretas, comprensibles y aplicables para organizaciones que no están completamente familiarizadas con estos conceptos. En lugar de abordar la nube únicamente como un conjunto de servicios técnicos, la

propuesta se entiende como un ecosistema que requiere gobierno, controles, procesos, roles, políticas, documentación y mejora continua.

La implementación del Azure Well-Architected Framework permite evaluar las cargas de trabajo existentes desde cinco dimensiones fundamentales: seguridad, confiabilidad, excelencia operacional, eficiencia de rendimiento y optimización de costos. Microsoft indica que el framework busca ayudar a mejorar las cargas de trabajo mediante recomendaciones asociadas a estos pilares. (Microsoft, 2026) Esta aproximación permite que la organización no se limite a corregir problemas aislados, sino que pueda construir una hoja de ruta integral de madurez cloud.

Finalmente, la propuesta de valor se materializa en una consultoría tecnológica que entrega diagnóstico, recomendaciones, arquitectura objetivo, modelo de gobierno, hoja de ruta de implementación y criterios de mejora continua. Esto permite que la organización pase de una adopción cloud reactiva y desordenada a un modelo de administración controlado, documentado, escalable y alineado con sus necesidades estratégicas.

## PERFIL DEL CLIENTE

El cliente objetivo es una organización pública que presenta una marcada obsolescencia tecnológica y que, como respuesta a necesidades operativas o estratégicas, ha decidido implementar soluciones en nube pública sin contar con un contexto previo suficiente sobre arquitectura cloud, modelos de servicio, tipos de recursos, seguridad, operación, costos y gobierno.

Este cliente posee infraestructura local heredada, aplicaciones antiguas, procesos manuales, documentación incompleta, baja estandarización técnica y una dependencia significativa de proveedores externos o equipos internos con conocimiento fragmentado. En muchos casos, la organización ha iniciado la adopción de Azure por proyectos puntuales, migraciones urgentes, necesidades de disponibilidad, reducción de infraestructura física o iniciativas de transformación digital, pero sin una planeación integral del modelo operativo cloud.

El perfil del cliente se caracteriza por tener múltiples recursos desplegados en Azure sin una estructura clara de administración. Cuenta con varias suscripciones, redes virtuales, máquinas virtuales, bases de datos, cuentas de almacenamiento, servicios PaaS y componentes de seguridad, pero sin una jerarquía de Management

Groups, sin políticas obligatorias, sin segmentación adecuada entre ambientes, sin control homogéneo de accesos y sin documentación actualizada de arquitectura.

También se trata de una organización que no cuenta con políticas internas suficientemente claras para guiar la implementación de soluciones cloud. Esto incluye ausencia de lineamientos de nombramiento, etiquetado, control de costos, gestión de identidades, segmentación de red, uso de regiones, configuración de respaldos, monitoreo, continuidad operativa, seguridad perimetral y revisión periódica de cumplimiento.

El cliente también puede presentar problemas de visibilidad y control. Al no existir un modelo de gobernanza formal, cada área, proveedor o administrador puede desplegar recursos según su propio criterio, generando duplicidad, sobrecostos, riesgos de seguridad y dificultades para auditar el entorno. Esta situación se vuelve más crítica cuando los recursos soportan procesos misionales, servicios ciudadanos, aplicaciones productivas o información sensible.

En términos de necesidades, este cliente requiere acompañamiento especializado para entender su estado actual, identificar riesgos, ordenar su arquitectura, definir políticas, construir una hoja de ruta y capacitar a sus equipos. No busca únicamente una implementación técnica, sino una guía metodológica que le permita adoptar la nube de manera más madura, segura y sostenible.

## MAPA DE VALOR

El mapa de valor de la solución se estructura a partir de los problemas, necesidades y expectativas de entidades públicas que han implementado servicios en Microsoft Azure sin una arquitectura previamente definida. Estas organizaciones requieren pasar de una administración reactiva de recursos cloud a un modelo gobernado, seguro, documentado y alineado con buenas prácticas de arquitectura. La propuesta busca generar valor mediante un servicio de consultoría tecnológica que combine diagnóstico, diseño de arquitectura, definición de lineamientos, priorización de brechas y transferencia de conocimiento. Desde la perspectiva del cliente, las principales necesidades se relacionan con obtener visibilidad sobre el estado real del entorno Azure, identificar riesgos técnicos, ordenar los recursos existentes, reducir costos innecesarios, proteger la información institucional, mejorar la disponibilidad de servicios digitales y establecer un modelo de gobierno que oriente futuras implementaciones. Estas necesidades son especialmente relevantes en entidades públicas donde los servicios tecnológicos soportan procesos misionales,

atención ciudadana, gestión documental, interoperabilidad, analítica de datos y operación administrativa. Los aliviadores de frustraciones de la propuesta se materializan en la reducción de incertidumbre técnica y operativa. Al entregar un diagnóstico claro, la entidad puede entender qué tiene desplegado, qué riesgos existen, qué recursos requieren intervención, qué configuraciones deben corregirse y qué acciones deben priorizarse. Esto permite disminuir el crecimiento descontrolado del entorno cloud y evitar que cada área o proveedor implemente soluciones bajo criterios aislados.

| **Elemento** | **Descripción** |
|---|---|
| Cliente objetivo | Entidades públicas con servicios Azure implementados sin arquitectura, gobernanza o documentación suficiente. |
| Necesidades | Ordenar el entorno cloud, reducir riesgos, mejorar seguridad, controlar costos, documentar soluciones y definir una hoja de ruta. |
| Dolores | Recursos dispersos, baja visibilidad, duplicidad, costos no controlados, ausencia de políticas, redes mal segmentadas y baja alfabetización cloud. |
| Producto principal | Consultoría de diagnóstico y gobierno de arquitectura cloud en Azure. |
| Servicios asociados | Evaluación WAF, arquitectura objetivo, Azure Policy, RBAC, Management Groups, segmentación de red, FinOps, monitoreo y documentación. |
| Aliviadores de dolor | Diagnóstico claro, priorización de brechas, reducción de riesgos, control de costos y estandarización técnica. |
| Generadores de valor | Madurez cloud, operación gobernada, seguridad por diseño, trazabilidad, cumplimiento y mejora continua. |

Tabla 1 Elementos Mapa de Valor

Los generadores de valor se evidencian en la capacidad de convertir la nube en un entorno administrable, auditable y escalable. La entidad obtiene una arquitectura más ordenada, mejores controles de seguridad, mayor visibilidad operativa, menor exposición a riesgos, mejor control financiero y una base documental que facilita auditorías, soporte, continuidad y evolución de servicios. Además, la transferencia de conocimiento permite que los equipos internos comprendan las buenas prácticas aplicadas y puedan sostenerlas en el tiempo. El mapa de valor evidencia que la propuesta tiene un encaje directo con las necesidades de entidades públicas que han adoptado nube sin suficiente madurez arquitectónica. El valor no se limita a la implementación técnica, sino que se concentra en construir capacidades institucionales para que la entidad pueda administrar sus recursos cloud de forma segura, eficiente, documentada y sostenible.

## ANÁLISIS DE LAS ALTERNATIVAS TÉCNICAS PARA SOLUCIONAR EL PROBLEMA

El Well-Architected Framework está diseñado para proveer los lineamientos de alto nivel con las mejores Prácticas para ayudar a mantener las aplicaciones confiables, seguras, con alto rendimiento, gestión del costo, y la excelencia operativa de los recursos de nube.

- Segmentación por tipo de recurso
- Segmentación de ambientes
- Estandarización de nomenclaturas.
- Ambientes homogéneos

La siguiente es la propuesta de reorganización de recursos para todas las suscripciones, esta propuesta está basada en las mejores prácticas del Well-Architected Framework de Azure teniendo en cuenta los principios aislamiento de recursos, diseño escalable y Control de Recursos.

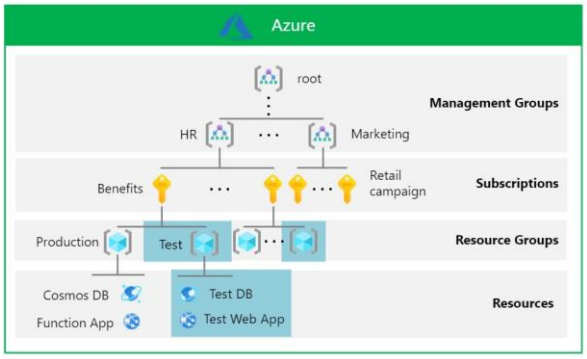


Ilustración 13 Propuesta de reorganización

### Nomenclatura de Nombramiento de Recursos

El Siguiente es el estándar de nombres que se debe utilizar de acuerdo con los componentes implementados:

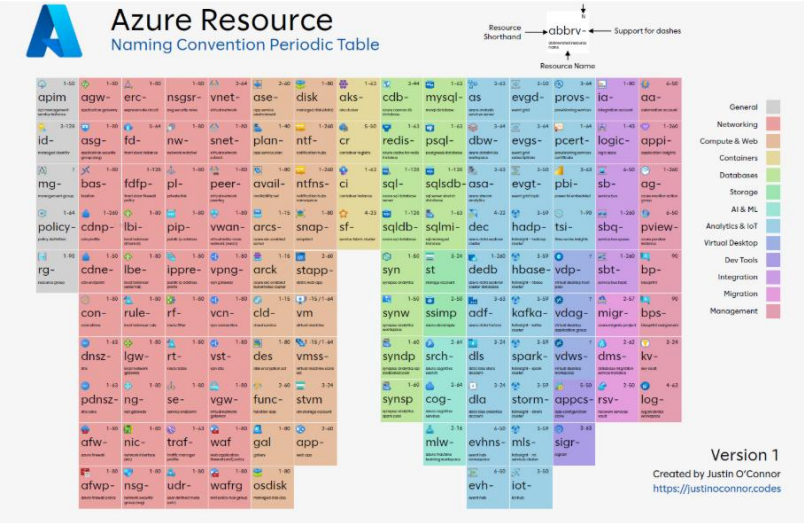

Ilustración 14 Tabla de convenciones de nombramiento

El siguiente es el formato que debe tener cada componente implementado, se debe dejar todo en minúscula:

- [az] – [tipo de componente]- [aplicación]– [suscripción]-[ambiente]-[identificador].
    - Un ejemplo para un componente tipo Máquina Virtual es: az-vm-app1-atencion-pro-001

**Privilegio de Acceso Mínimo**

El principio de mínimo privilegio es un concepto clave en la seguridad, que establece que los usuarios, aplicaciones y servicios deben tener solo los privilegios necesarios para realizar su trabajo. Este principio es esencial para reducir la superficie de ataque y minimizar los riesgos de accesos no autorizados o mal uso de recursos

Azure proporciona el modelo de Control de Acceso Basado en Roles (RBAC) donde se pueden realizar la personalización de permisos por roles y detallar las acciones que cada usuario puede realizar con los recursos de Azure, se debe evitar la asignación de permisos de Administrador general para asegurar la aplicación de las mejores prácticas en la asignación de permisos.

## MODELO DE NEGOCIO

Se orienta a la prestación de servicios de consultoría tecnológica especializada en diagnóstico, arquitectura, gobernanza y optimización de entornos Microsoft Azure. La solución está dirigida a organizaciones públicas que ya han implementado servicios en nube pública, pero que requieren acompañamiento para ordenar, documentar, asegurar y optimizar su arquitectura cloud.

Este modelo se fundamenta en la entrega de valor mediante conocimiento especializado, análisis técnico, definición de buenas prácticas, documentación arquitectónica y acompañamiento en la implementación de controles. A diferencia de un modelo centrado únicamente en la venta o despliegue de infraestructura, la propuesta se enfoca en el diagnóstico y la maduración del entorno existente.

La propuesta puede ser ofrecida como un servicio profesional por proyecto, por paquete de diagnóstico o mediante acompañamiento continuo. En organizaciones con baja madurez cloud, el primer entregable puede ser una evaluación integral del estado actual. En organizaciones con mayor avance, el servicio puede evolucionar hacia el diseño de landing zones, implementación de políticas, segmentación de redes, optimización de costos o fortalecimiento de seguridad.

## PROPUESTA DE MODELO DE NEGOCIO

La propuesta de modelo de negocio se basa en un servicio de consultoría tecnológica denominado, de forma conceptual, Diagnóstico y Gobierno de Arquitectura Cloud en Azure. Este servicio tiene como objetivo ayudar a organizaciones con adopciones cloud desordenadas a construir una arquitectura gobernada, segura, documentada y optimizada.

- Segmento de clientes: organizaciones públicas con recursos desplegados en Azure, múltiples suscripciones activas, baja madurez cloud, obsolescencia tecnológica, ausencia de documentación, problemas de costos, riesgos de seguridad o falta de estándares de arquitectura.
- Propuesta de valor: diagnóstico técnico y metodológico del entorno Azure, identificación de brechas frente al Azure Well-Architected Framework, diseño de un modelo de gobernanza cloud y definición de una hoja de ruta de implementación priorizada
- Canales: venta directa consultiva, alianzas con proveedores cloud, participación en procesos de contratación pública, presentación de

propuestas técnicas, referencias profesionales y oferta de servicios especializados a áreas de tecnología, arquitectura empresarial, seguridad o transformación digital.

- Relación con clientes: acompañamiento consultivo, trabajo colaborativo con equipos internos, sesiones de levantamiento, talleres de arquitectura, presentación de hallazgos, validación de brechas y definición conjunta de prioridades.
- Fuentes de ingreso: proyectos de diagnóstico, paquetes de arquitectura, consultoría por horas, acompañamiento mensual, implementación de políticas, diseño de landing zones, documentación técnica y capacitación especializada.
- Recursos clave: consultores cloud, arquitectos Azure, especialistas en seguridad, conocimiento en WAF, CAF, networking, gobierno cloud, Azure Policy, RBAC, FinOps, documentación técnica y gestión de proyectos.
- Actividades clave: levantamiento de información, análisis técnico, entrevistas con equipos, revisión de suscripciones, evaluación de arquitectura, diseño de lineamientos, priorización de brechas, elaboración de entregables y presentación ejecutiva de resultados.
- Estructura de costos: horas de consultoría, herramientas de análisis, documentación, licenciamiento si aplica, capacitación, gestión del proyecto y costos administrativos asociados a la prestación del servicio.

## VALIDACIÓN DEL MODELO DE NEGOCIO

La validación del modelo de negocio puede realizarse mediante una estrategia progresiva basada en evidencia técnica y retroalimentación del cliente. En una primera etapa, se puede aplicar un diagnóstico cloud de alcance limitado sobre una o dos suscripciones representativas, con el fin de identificar brechas visibles en gobernanza, seguridad, costos, nomenclatura, documentación y segmentación de red. Este diagnóstico inicial permitiría validar si la organización reconoce valor en los hallazgos presentados y si las recomendaciones son accionables dentro de su contexto técnico y presupuestal. La validación no debe centrarse únicamente en la aceptación comercial del servicio, sino también en la capacidad de demostrar mejoras concretas, tales como reducción de riesgos, identificación de recursos innecesarios, mejora de cumplimiento de políticas, reducción de exposición pública o definición de una hoja de ruta clara.

Una segunda forma de validación consiste en realizar talleres con equipos técnicos y directivos para contrastar los hallazgos frente a las necesidades reales de la

organización. Estos espacios permiten validar si el lenguaje utilizado es comprensible para equipos con baja alfabetización cloud y si la propuesta logra traducir conceptos complejos de arquitectura en decisiones prácticas de operación. También se puede validar el modelo mediante indicadores antes y después de la intervención. Algunos indicadores útiles son: porcentaje de recursos con tags obligatorios, número de recursos sin propietario, cantidad de NSG sin uso, cumplimiento de Azure Policy, Secure Score, cantidad de recursos expuestos públicamente, costos mensuales por suscripción, número de recursos huérfanos, existencia de documentación actualizada y adopción de estándares de nomenclatura. El modelo se valida si la organización logra pasar de una administración reactiva de recursos cloud a una administración basada en gobierno, arquitectura, seguridad y mejora continua. En ese sentido, el éxito del modelo no se mide únicamente por la entrega de documentos, sino por la capacidad de generar decisiones técnicas más ordenadas, sostenibles y alineadas con los objetivos de la organización.

## PROPUESTA DE LA SOLUCIÓN TECNOLÓGICA

La propuesta esta orientada a evolucionar la jerarquía actual de Management Groups (Tenant Root Group y Administrator) hacia una estructura alineada con el CAF Enterprise-Scale. Como acción inmediata y a medida que se implementa la jerarquía recomendada a continuación, es importante que las suscripciones actualmente bajo Tenant Root Group se muevan al árbol de Administrator para garantizar la cobertura completa de las políticas de Azure Policy.

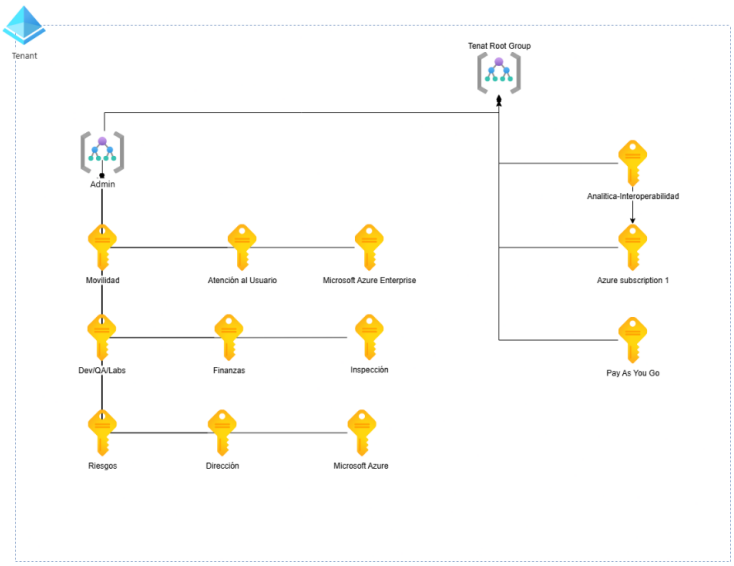


Ilustración 15 Distribución de Suscripciones

El siguiente es un ejemplo de esta segmentación a nivel de red y la agrupación de los componentes por cada una de ellas:

| **Componente** | **Servicios** |
|---|---|
| **Azure VNet** | |
| Subnet 1: Compute (VMs / AKS) | NSG, VM Scale Sets, AKS |
| Subnet 2: Databases | Azure SQL, CosmosDB, MySQL / Private Link |
| Subnet 3: Web Apps | Azure App Services / Azure App Gateway (WAF) |
| Subnet 4: Monitoring | Azure Monitor, Log Analytics |
| Subnet 5: Gestión y Seguridad | VPN Gateway, Azure Firewall / Azure Bastion |

Tabla 2 Segmentación de red

La siguiente es la nueva distribución de las suscripciones, de acuerdo con el proceso de reorganización de componentes de Cloud y alineamiento con las mejores prácticas de WAF de Azure.

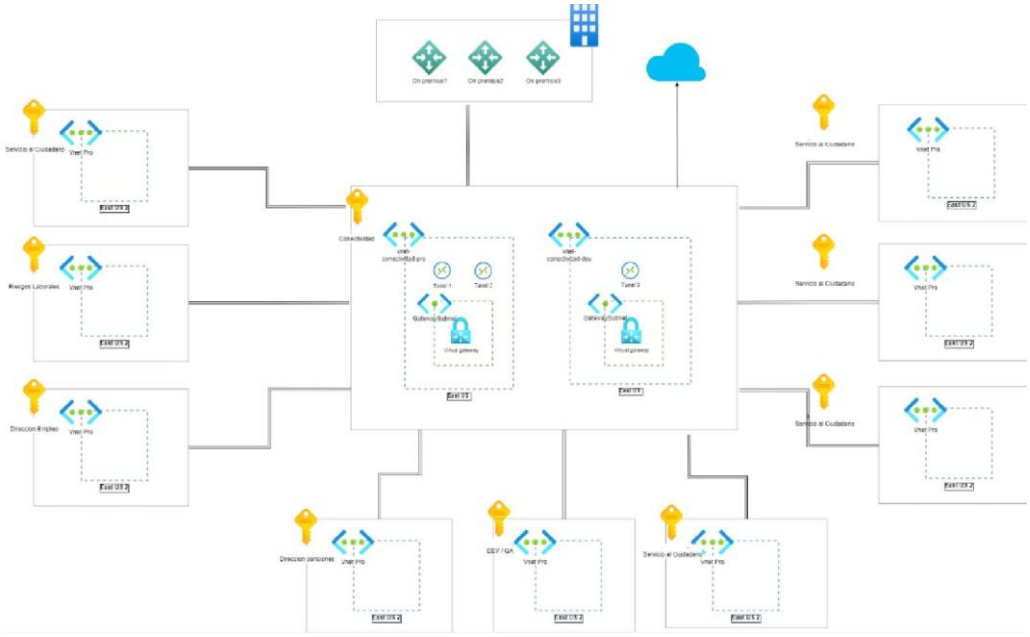

Ilustración 16 Arquitectura Hub & Spoke Final

## Networking

La distribución de las redes implementadas en Azure, la segmentación por componentes funcionales se realizó a nivel de subredes, cada suscripción tiene el mismo esquema básico para poder realizar la segmentación de las soluciones y tener el control del networking, este diseño se realizó teniendo en cuenta los principios de eficiencia del rendimiento, y la excelencia operativa.

El tenant cuenta con 30 Virtual Networks distribuidas en 9 suscripciones. Se ha realizado una reorganización con 9 VNets que siguen un estándar de nombrado (az-vnet--001) y rangos de direccionamiento planificados. Adicionalmente, coexisten 21 VNets legacy, de las cuales 18 presentan solapamiento crítico de direcciones IP, y 3 no presentan conflicto de direccionamiento directamente. Se crea una VNet Hub (AZ_VNET_HUB_01) con espacios de red 10.20.x.x/24, 10.20.x.x/24, 10.20.x.x/24, y 10.20.x.x/24 en una de las suscripciones, y una VNet de conectividad (az-vnet conectividad-001) con rango 10.99.x.x/24 en la suscripción de Conectividad. Además, se han creado 9 VNets con naming estandarizado y rangos planificados.

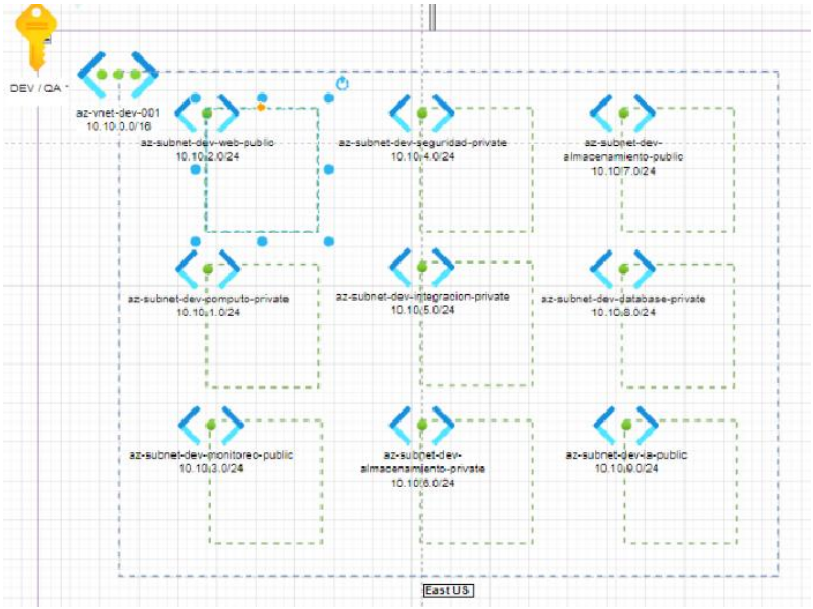


Ilustración 17 Reorganización de vnet

En el entorno a intervenir se ha iniciado con un proceso de reorganización de su infraestructura en Azure. Se ha creado una suscripción dedicada a conectividad y se ha comenzado a estandarizar el nombrado de VNets con el patrón az-vnet--001 con rangos /16 planificados sin solapamiento. Sin embargo, aún coexisten 21 VNets legacy con nomenclatura inconsistente, direcciones IP solapadas, y sin integración

al modelo Hub & Spoke. La transición debe completarse para alinear el entorno con el CAF. El modelo está basado en la topología Hub and Spoke, donde se tiene una suscripción de conectividad que centraliza todos los recursos transversales de red y las conexiones entre suscripciones para evitar la propagación de peerings entre suscripciones y perder el control de la correcta administración del tráfico y la comunicación entre Azure y On premises.

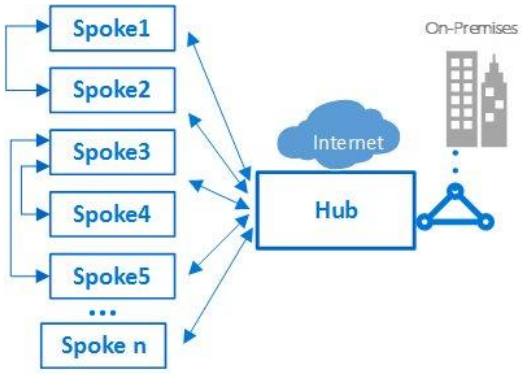


Ilustración 18 Hub & Spoke

**Segmentación de Seguridad**

El siguiente es modelo de segmentación por capas que está basado en el pilar de seguridad, teniendo en cuenta que los componentes se desplegaran en diferentes subredes, se deben utilizar los Componentes de agrupación Lógica ( Grupo de recursos ) para la agrupación de todos los componentes que hacen parte de la solución, y se deben implementar los componentes de control de tráfico ( Grupos de seguridad de red y grupos de seguridad de aplicación ) para asegurar la comunicación exclusiva de los componentes de la solución implementada.

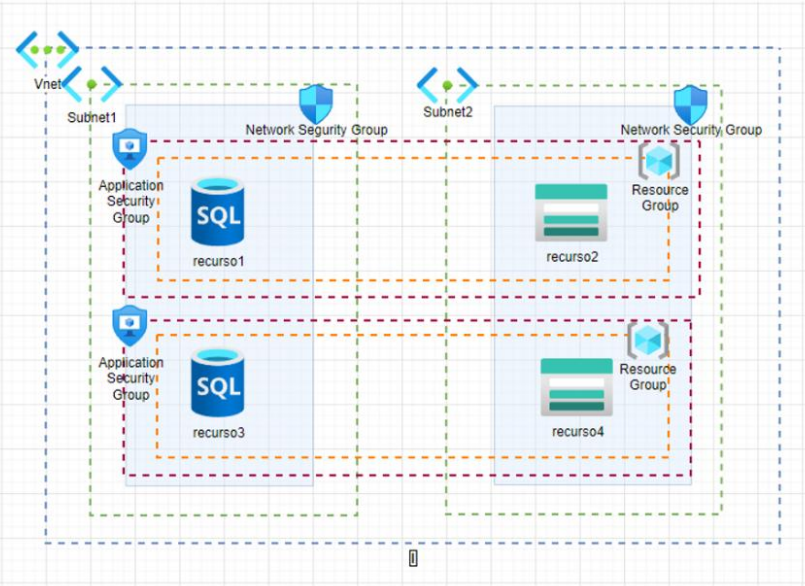


Ilustración 19 Segmentación de seguridad

Todas las soluciones implementadas deben realizar la implementación de Endpoints privados en la mayoría de los recursos posibles, teniendo en cuenta el pilar de seguridad del Well-Architected Framework de Azure.

La implementación de Private Endpoint se ha enfocado en mejorar la seguridad de las soluciones implementadas en Azure, ya que permiten la comunicación privada de recursos evitando la exposición de datos públicos. La implementación de Private Endpoint debe ser tomada como una de las mejores prácticas de arquitectura para garantizar soluciones más seguras y acordes a los lineamientos públicos del Well-Architected Framework de Azure.

Dado el contexto anterior se realizan las siguientes actividades:

- Asignación de tablas de enrutamiento a todas las subnets de Suscripción de Atención al Usuario de forma inmediata. Es la brecha más crítica identificada en la segmentación de red.
- Se completa la asignación de tablas de enrutamiento en las subnets faltantes (subnets de integracion-private, almacenamiento-private y almacenamiento public).
- Ampliar el espacio de direccionamiento de az-vnet-conectividad-001 de /24 a un rango mayor (ej: 10.99.0.0/22) y crear las subnets de Hub faltantes:

AzureFirewallSubnet (mínimo /26), AzureBastionSubnet (mínimo /26), y una subnet de gestión/DNS.

- Crear una subnet dedicada para Private Endpoints en cada VNet spoke (ej: az-subnet-privateendpoints, rango 10.X.X.0/24) para centralizar los endpoints privados de servicios PaaS.
- Auditar las reglas de los NSGs de las subnets clasificadas como “public” para asegurar que no permitan tráfico directo desde Internet sin pasar por un Application Gateway o Azure Front Door.
- Validar que todas las Route Tables fuerzan el tráfico 0.0.0.0/0 al Azure Firewall del Hub (next hop type: Virtual Appliance) para garantizar inspección centralizada del tráfico saliente.
- Se ha configurado el envío de Activity Logs al Log Analytics workspace mediante política.
- Se ha habilitado el monitoreo de VMs con Azure Monitoring Agent (AMA) mediante iniciativa (en Preview).
- La iniciativa de tags obligatorios requiere validación de que los tags están efectivamente aplicados en todos los recursos existentes mediante una tarea de remediación (cumplimiento actual de 94%).

De acuerdo con el contexto anterior se pudo realizar la implementación de suscripciones que cumplen con los estándares definidos en el WAF, se ha realizado la reorganización tanto de grupos de recursos, suscripciones y soluciones completas dentro del tenant de Azure. A continuación, se presentan los resultados a nivel de arquitectura de las soluciones intervenidas.

Se realiza la reorganización a nivel de conectividad de manera independiente para cada suscripción, segmentando los componentes de acuerdo con su criticidad y tipo, garantizando su categorización de manera adecuada y sin afectar el funcionamiento de estas. En los siguientes diagramas se observa la categorización por tipo de solución en cada grupo de recursos y su segmentación a nivel de red por tipo de componente.

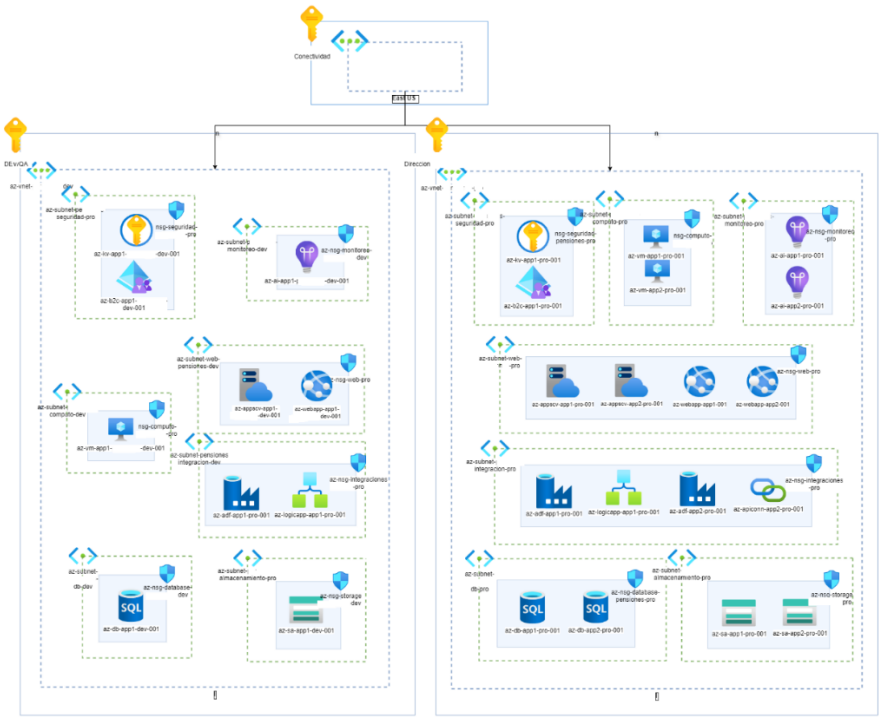

Ilustración 20 Suscripción intervenida 1 - segmentación de componentes

Garantizando así una comunicación adecuada entre cada componente, solución, grupo de recursos y sin generar conflictos a nivel de conectividad.

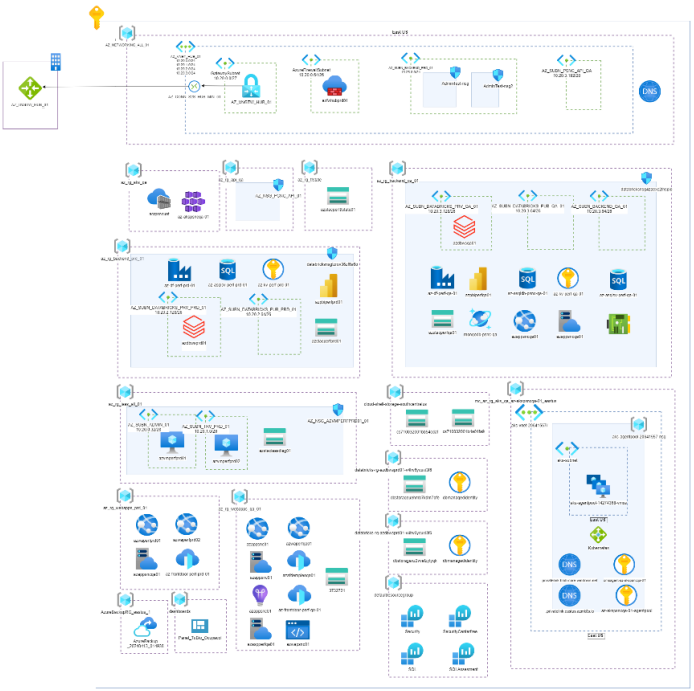

Ilustración 21 Suscripción intervenida 2 - segmentación de componentes

Garantizando espacios de replicación o backup en caso de desastres o indisponibilidades, apuntando a servicios con alta disponibilidad y resiliencia tecnológica.

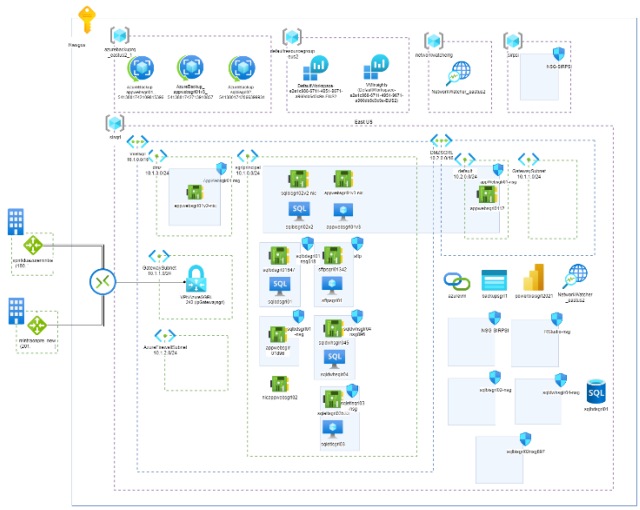

Ilustración 22 Suscripción intervenida 4 - segmentación de componentes

Aplicando cada capa de seguridad para cada tipo de componente se reducen los riesgos identificados durante el diagnóstico y asegura la integridad de la información que es alojada en los recursos aprovisionados dentro del tenant de Azure.

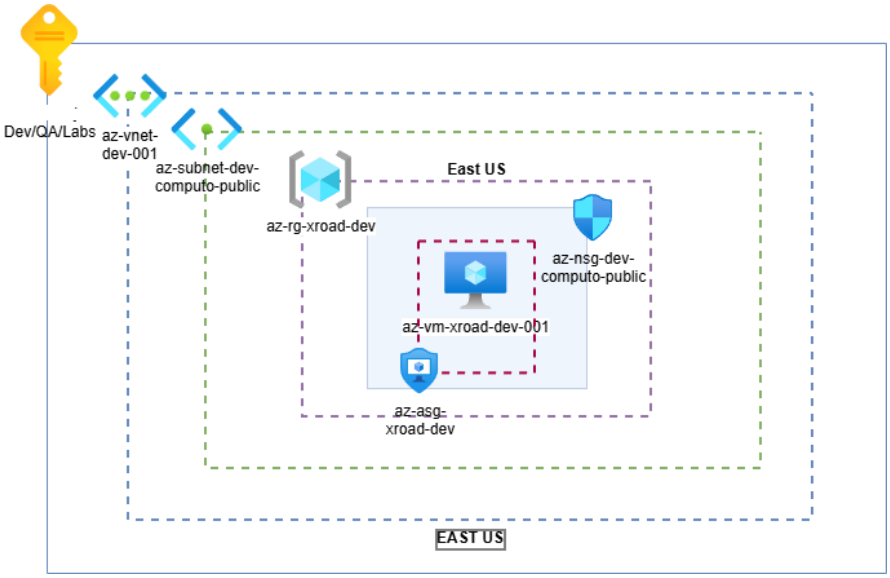


Ilustración 23 Segmentación completa a solución

Durante todo el proceso de implementación se plantearon sesiones técnicas con las áreas funcionales donde se categorizaba la criticidad de cada una de sus soluciones y la importancia de mantener los servicios operativos y funcionales. De igual forma se plantearon escenarios de diagnostico y entregas documentales denominadas líneas base, donde describíamos el estado actual por solución y acciones de mejora que podrían ser implementadas a corto plazo sin afectar la disponibilidad de los recursos.

Posteriormente se plantearon escenarios de priorización y planeación para cada suscripción o solución, generando espacio de capacitación y alfabetización tecnológica y cloud para los directamente involucrados en el proceso desde la organización. Este ejercicio permitió que la organización pudiera investigar, indagar y construir de la mano de los diagnósticos y experiencia adquirida en el proceso, políticas de gobernanza que le permitirían a futuro implementar nuevas soluciones, plantear acciones de mejora continua y estandarizar las implementaciones de proyectos tanto de desarrollo interno como de desarrollo externo o tercerizado.

## ANÁLISIS DEL PROCESO DE TRANSFORMACIÓN DIGITAL

El proceso de transformación digital abordado en esta propuesta no debe entenderse únicamente como la migración o implementación de recursos tecnológicos en Microsoft Azure. Para una entidad pública, la transformación digital implica modificar la forma en que se diseñan, operan, gobiernan y mejoran los servicios institucionales apoyados en tecnología. En este sentido, la adopción de nube pública representa un habilitador, pero no constituye por sí misma una transformación si no está acompañada de gobierno, arquitectura, seguridad, gestión del cambio, documentación y medición de resultados.

La Política de Gobierno Digital establece que la transformación digital pública busca generar valor público, fortalecer la relación entre ciudadano y Estado, mejorar la prestación de servicios y aumentar la confianza en las instituciones mediante el uso y aprovechamiento de las TIC. Por tanto, cualquier iniciativa de nube pública en entidades estatales debe alinearse con objetivos institucionales y no limitarse a decisiones puramente técnicas. ( Ministerio de Tecnologías de la Información de Colombia, 2026). El punto de partida corresponde a una entidad que ha implementado recursos en Azure sin una arquitectura previamente definida. Esta situación refleja una primera etapa de adopción digital caracterizada por la urgencia operativa: se despliegan suscripciones, máquinas virtuales, redes, bases de datos, servicios PaaS o cuentas de almacenamiento para resolver necesidades puntuales,

pero sin un modelo integral de gobierno. Como consecuencia, el entorno crece de manera fragmentada, con baja visibilidad transversal, duplicidad de recursos, inconsistencias de nomenclatura, debilidades de seguridad y dificultades para controlar costos.

1. La intervención propuesta transforma este escenario inicial mediante la adopción de buenas prácticas del Azure Well-Architected Framework y del Cloud Adoption Framework. El primer cambio consiste en pasar de una lógica de despliegue aislado a una lógica de arquitectura gobernada. Esto implica diagnosticar el estado actual, identificar brechas, clasificar recursos, definir estándares, establecer políticas, organizar suscripciones, segmentar redes y construir una hoja de ruta de mejora. Microsoft señala que el Well-Architected Framework puede mejorar la calidad de una carga de trabajo al ayudarla a ser resiliente, segura, rentable, operable responsablemente y capaz de cumplir su propósito dentro de tiempos aceptables.
2. El segundo cambio se presenta en la gobernanza institucional de la tecnología. La entidad deja de depender exclusivamente de decisiones individuales de administradores, proveedores o áreas aisladas, y comienza a operar bajo reglas comunes. Estas reglas pueden incluir estructuras de Management Groups, definición de roles y permisos, políticas de nomenclatura, tags obligatorios, restricciones de regiones, control de SKUs, lineamientos de backup, reglas de seguridad, monitoreo centralizado y validación de cumplimiento. Azure Policy ayuda a reforzar convenciones de seguridad y administración en entornos Azure, complementando RBAC y apoyando la gestión de costos.
3. El tercer cambio corresponde a la seguridad y privacidad de la información. En una entidad pública, los recursos cloud pueden soportar datos sensibles, trámites, servicios ciudadanos, información misional o integraciones con otros sistemas. Por ello, la transformación digital debe incorporar seguridad desde el diseño, no como una actividad posterior. El MSPI orienta a las entidades públicas para incorporar seguridad de la información en procesos, trámites, servicios, sistemas, infraestructura y activos de información, preservando confidencialidad, integridad, disponibilidad y privacidad de los datos.
4. El cuarto cambio se relaciona con la operación y la continuidad. Un entorno Azure gobernado permite mejorar la capacidad de monitoreo, respuesta ante incidentes, trazabilidad, auditoría y recuperación. La consolidación de logs, la implementación de alertas, el uso de Azure Monitor, Log Analytics, Microsoft Defender for Cloud, respaldos y segmentación de red contribuyen

a que los servicios digitales puedan operar con mayor estabilidad. Esto es relevante porque la transformación digital pública busca mejorar la entrega de servicios y mantener la confianza de los ciudadanos en la capacidad institucional del Estado.

El proceso de transformación digital puede representarse en cuatro fases principales. La primera fase es el diagnóstico, donde se levanta el estado actual del entorno Azure y se identifican brechas. La segunda fase es el diseño, donde se define la arquitectura objetivo, los lineamientos de gobernanza y la hoja de ruta. La tercera fase es la implementación progresiva, donde se aplican políticas, segmentación, controles de acceso, monitoreo y ajustes de costos. La cuarta fase es la mejora continua, donde se miden indicadores, se revisa cumplimiento, se actualiza documentación y se ajustan controles de acuerdo con nuevas necesidades institucionales.

| **Fase** | **Actividades principales** | **Resultado esperado** |
|---|---|---|
| Diagnóstico | Inventario, revisión de suscripciones, redes, seguridad, costos, políticas y documentación. | Identificación de brechas y riesgos. |
| Diseño | Arquitectura objetivo, modelo de gobernanza, estándares, políticas y hoja de ruta. | Modelo cloud estructurado y priorizado. |
| Implementación | Aplicación de controles, segmentación, RBAC, Azure Policy, monitoreo y optimización. | Entorno Azure más seguro, ordenado y gobernado. |
| Mejora continua | Medición, remediación, actualización documental, capacitación y revisión periódica. | Madurez cloud sostenible en el tiempo. |

Tabla 3 Fases del Proceso de Transformación Digital

Como resultado, la transformación digital generada por la propuesta no se limita a una mejora técnica puntual, sino que habilita una nueva forma de administrar la nube dentro de la entidad. La organización pasa de una operación reactiva a un modelo basado en arquitectura, gobierno, seguridad, control financiero, documentación y aprendizaje institucional. Esto permite que futuras soluciones digitales se implementen sobre una base más sólida, reduciendo riesgos y aumentando la capacidad de la entidad para prestar servicios confiables, seguros y sostenibles.

## ASPECTOS LEGALES Y CONTRATACIÓN

Para el sector público, la implementación de un modelo de diagnóstico, arquitectura y gobernanza cloud en Microsoft Azure debe analizarse no solo desde una perspectiva técnica, sino también desde el marco legal, contractual, presupuestal y de cumplimiento aplicable a las entidades estatales. La contratación de servicios asociados a nube pública, consultoría tecnológica, seguridad de la información y acompañamiento especializado debe observar los principios de la contratación estatal, la protección de datos personales, la seguridad digital, la planeación y la adecuada supervisión contractual. En Colombia, el marco general de la contratación estatal se fundamenta en la Ley 80 de 1993, por medio de la cual se expide el Estatuto General de Contratación de la Administración Pública, y en la Ley 1150 de 2007, que introduce medidas para la eficiencia y la transparencia en la contratación con recursos públicos. Estas normas son relevantes para la propuesta porque cualquier contratación de servicios de consultoría tecnológica o nube pública por parte de una entidad estatal debe estructurarse bajo criterios de selección objetiva, planeación, responsabilidad, economía y transparencia. (Función Pública, 1993).

La entidad debe definir adecuadamente el objeto contractual. Para esta propuesta, el objeto no debería limitarse a “adquirir servicios de Azure” o “contratar servicios de nube”, ya que el alcance real corresponde a un servicio especializado de diagnóstico, arquitectura, gobernanza, seguridad y optimización de un entorno Azure existente.  En la etapa precontractual, la entidad debe elaborar estudios previos que justifiquen la necesidad, el alcance, la modalidad de contratación, los riesgos, el presupuesto, los criterios técnicos habilitantes y los entregables esperados. En este tipo de proyecto, la justificación debe apoyarse en la necesidad de fortalecer la seguridad, mejorar la disponibilidad de servicios digitales, reducir riesgos operativos, optimizar costos cloud, documentar la arquitectura existente, establece. Respecto al mecanismo de contratación, las entidades públicas pueden acudir a los instrumentos disponibles según la naturaleza del servicio, el presupuesto, la modalidad aplicable y la normatividad vigente. Para servicios de nube pública, Colombia Compra Eficiente cuenta con acuerdos marco y mecanismos de agregación de demanda. El Acuerdo Marco de Precios de Servicios de Nube Pública V tiene por objeto seleccionar proveedores de servicios de nube pública y definir condiciones para que las entidades estatales contraten estos servicios, incluyendo condiciones para el pago. (Agencia Nacional de Contratación Pública CCE, 2026) Sin embargo, debe distinguirse entre la adquisición de consumo cloud y la contratación de consultoría especializada, ya que algunos acuerdos marco pueden excluir consultorías o servicios no contemplados dentro del objeto

específico del instrumento. El Sistema Electrónico para la Contratación Pública —SECOP— es el medio oficial de información de toda la contratación realizada con dineros públicos y constituye el punto único de ingreso de información para entidades que contratan con cargo a recursos públicos. SECOP II, además, funciona como plataforma transaccional para gestionar en línea los procesos de contratación. Por ello, los documentos del proceso, estudios previos, pliegos, observaciones, contratos, modificaciones y documentos de ejecución deben publicarse y gestionarse conforme a los lineamientos aplicables. (Agencia Nacional de Contratación Pública CCE, 2026)

En materia de protección de datos personales, la Ley 1581 de 2012 establece disposiciones generales aplicables a datos personales registrados en bases de datos susceptibles de tratamiento por entidades públicas o privadas. Esta ley desarrolla derechos constitucionales relacionados con conocer, actualizar y rectificar información personal recogida en bases de datos o archivos. (Función Pública, 2012). En consecuencia, si durante el diagnóstico o intervención se accede a información personal, metadatos, configuraciones, bases de datos o registros que puedan contener datos personales, el contrato debe incluir obligaciones de confidencialidad, tratamiento adecuado de información, limitación de acceso, reserva y cumplimiento de políticas internas de protección de datos.

En seguridad de la información, la entidad debe alinear el proyecto con el Modelo de Seguridad y Privacidad de la Información —MSPI—. En 2025, MinTIC actualizó el MSPI mediante la Resolución 02277 de 2025, adoptando lineamientos alineados con ISO/IEC 27001:2022 y fortaleciendo la estrategia de seguridad digital del Estado colombiano. Este modelo busca garantizar confidencialidad, integridad, disponibilidad y privacidad de la información en el sector público (Ministerio de Tecnológias de la Información, 2025). Por tanto, la consultoría debe considerar controles de acceso, gestión de identidades, clasificación de activos, gestión de riesgos, monitoreo, continuidad, seguridad en nube y relación con proveedores tecnológicos. Finalmente, la contratación debe incluir mecanismos de supervisión y seguimiento. El supervisor del contrato debe verificar el cumplimiento técnico, administrativo, financiero y documental del proyecto. Para ello, se recomienda establecer reuniones periódicas, actas de seguimiento, validación de entregables, matriz de compromisos, control de riesgos, cronograma de actividades y evidencias de capacitación. La adecuada supervisión permite garantizar que la consultoría no se quede en recomendaciones generales, sino que produzca insumos aplicables para mejorar el entorno Azure de la entidad.

# CONCLUSIONES

La implementación del Azure Well-Architected Framework en un entorno multi-suscripción permite concluir que la adopción de nube pública requiere mucho más que el despliegue de recursos tecnológicos. En el caso analizado, la existencia de múltiples suscripciones, redes virtuales legacy, recursos sin estandarización, baja documentación, controles de seguridad parciales y ausencia de una arquitectura común evidencia que el principal reto no es únicamente técnico, sino de gobernanza, operación y madurez organizacional.

El diagnóstico realizado confirma la necesidad de establecer un modelo de gobierno cloud basado en políticas, roles, segmentación, monitoreo, documentación y control de costos. La propuesta de reorganización mediante Management Groups, Azure Policy, RBAC, modelo Hub & Spoke, Private Endpoints, Route Tables y estándares de nomenclatura permite construir una arquitectura más ordenada, segura y auditable, reduciendo los riesgos asociados al crecimiento descontrolado del entorno Azure.

Desde la perspectiva del sector público, la gobernanza cloud adquiere una importancia estratégica, ya que las soluciones tecnológicas suelen soportar procesos misionales, servicios ciudadanos, información sensible y operaciones críticas. Por esta razón, la aplicación del Well-Architected Framework contribuye no solo a mejorar la arquitectura técnica, sino también a fortalecer la transformación digital institucional, la continuidad operativa y la confianza en los servicios digitales.

Los cinco pilares del WAF deben entenderse como dimensiones interdependientes. Mejorar la confiabilidad, la seguridad o el rendimiento puede implicar mayores costos, mientras que optimizar costos de forma excesiva puede afectar disponibilidad o protección. Por tanto, el framework no debe aplicarse como una lista de chequeo, sino como una hoja de ruta gradual basada en criticidad, riesgos, presupuesto y objetivos institucionales.

Finalmente, el proyecto demuestra que la madurez cloud depende también de la alfabetización tecnológica de los equipos internos. La transferencia de conocimiento, la documentación de línea base, la definición de políticas y la mejora continua son elementos esenciales para que la organización pueda sostener el modelo propuesto en el tiempo. En consecuencia, el Azure Well-Architected Framework debe ser asumido como una práctica permanente de gobierno y evolución cloud, no como una intervención puntual.

## Referencias


Ministerio de Tecnologías de la Información de Colombia. (08 de 05 de 2026). *Política de Gobierno Digital*. Obtenido de Política de Gobierno Digital: https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

Agencia Nacional de Contratación Pública CCE. (05 de 03 de 2026). *Acuerdo Marco de Precios (AMP/SDA) de Servicios de de Nube Pública V.* Obtenido de Acuerdo Marco de Precios (AMP/SDA) de Servicios de de Nube Pública V.: https://www.colombiacompra.gov.co/archivos/portfolio-item/acuerdo-marco-de-precios-amp-sda-de-servicios-de-de-nube-publica-v?utm_source=chatgpt.com

Agencia Nacional de Contratación Pública CCE. (2026). *SECOP*. Obtenido de Sistema Electrónico para la Contratación Pública: https://www.colombiacompra.gov.co/secop

Función Pública. (28 de 10 de 1993). *Ley 80 de 1993*. Obtenido de Ley 80 de 1993: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=304

Función Pública. (17 de 10 de 2012). *Ley 1581 de 2012*. Obtenido de Ley 1581 de 2012: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Microsoft. (2023). *Cloud Adoption Framework for Azure. Microsoft Learn*. Obtenido de Cloud Adoption Framework for Azure. Microsoft Learn: https://learn.microsoft.com/en-us/azure/architecture/framework/

Microsoft. (2023). *Implement governance across multiple Azure subscriptions. Microsoft Learn.* Obtenido de Implement governance across multiple Azure subscriptions. Microsoft Learn.: https://learn.microsoft.com/en-us/azure/governance/management-groups/overview

Microsoft. (19 de 12 de 2025). *Management groups*. Obtenido de Management groups: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/resource-org-management-groups

Microsoft. (2026). *Azure Well-Architected Framework*. Obtenido de Azure Well-Architected Framework: https://learn.microsoft.com/en-us/azure/well-architected/

Microsoft. (2026). *Azure Well-Architected Review*. Obtenido de Microsoft Assessments: https://learn.microsoft.com/en-us/assessments/azure-architecture-review/

Microsoft. (2026). *What is cloud computing?* Obtenido de Cloud computing defined: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing

Ministerio de Tecnológias de la Información. (21 de 04 de 2025). *MSPI*. Obtenido de Modelo de Seguridad y Privacidad de la Información: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Ministerio de Tecnologias de la Información de Colombia. (2023). *Estrategia Nacional Digital de Colombia 2023-2026.* Obtenido de Estrategia Nacional Digital de Colombia 2023-2026: https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf

## LISTA DE FIGURAS



## LISTA DE TABLAS