



# TOGAF – Fases Preliminar y A

**Aplicación práctica en Banco Digital Seguro S.A.S.**

Un enfoque innovador para la arquitectura de ciberseguridad en fintech



# Transformando la Seguridad Bancaria

## Objetivo Principal

Implementar TOGAF (Fases Preliminar y A) para crear una arquitectura de ciberseguridad robusta y escalable

## Metodología

4 expertos especializados • 10 minutos cada uno • Enfoque práctico y colaborativo

## Caso de Estudio

Fintech "Banco Digital Seguro" - De startup a líder en seguridad bancaria digital

# Hoja de Ruta de la Presentación

01

## Contexto TOGAF y ADM

Fundamentos del marco arquitectural empresarial

02

## Fase Preliminar – Preparación

Establecimiento de bases y principios arquitecturales

03

## Fase A – Visión de la Arquitectura

Desarrollo de la visión estratégica de seguridad

04

## Caso Práctico

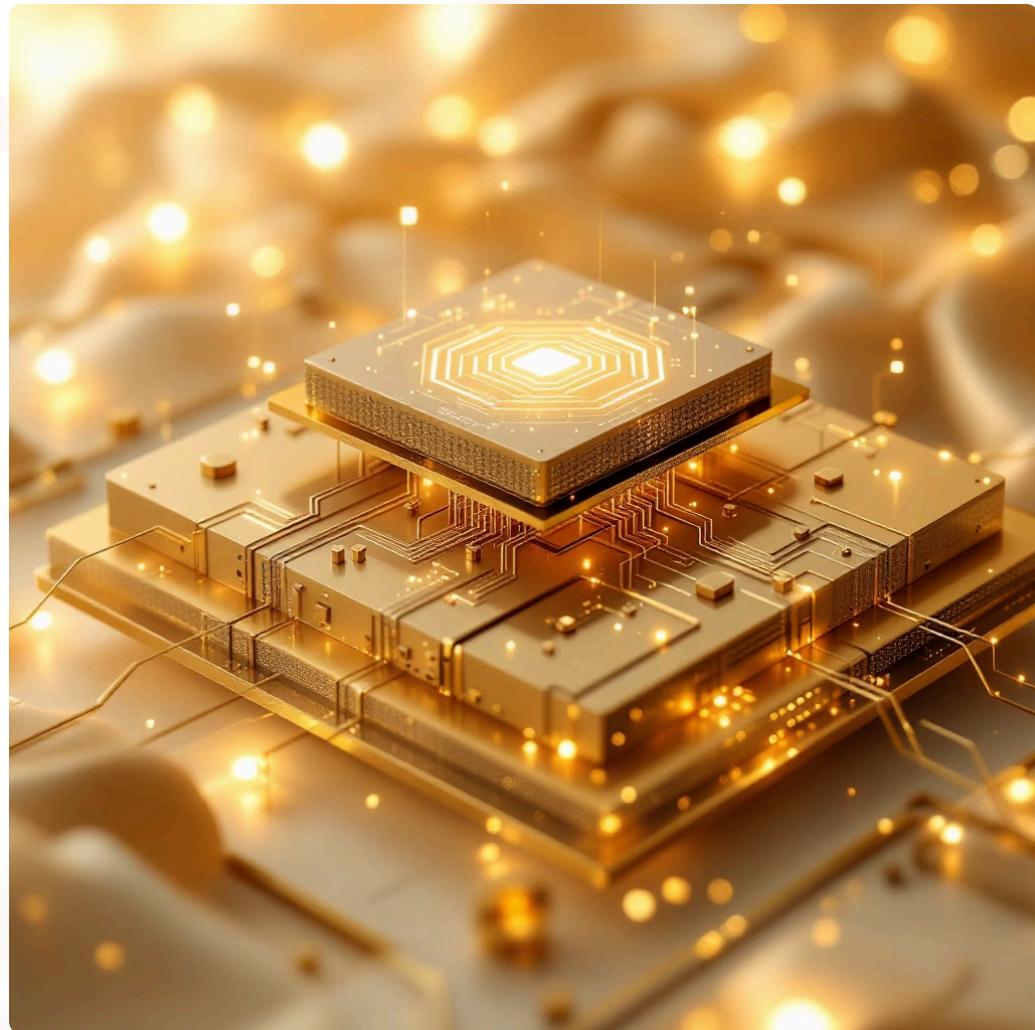
Implementación real en Banco Digital Seguro

05

## Diagramas, Roadmap y Conclusiones

Visualización de resultados y próximos pasos

# TOGAF: El Marco Arquitectural del Futuro



## ¿Qué es TOGAF?

**The Open Group Architecture Framework** - El estándar global para arquitectura empresarial que transforma la manera de diseñar sistemas seguros.

## ADM:

El **Architecture Development Method** es el **método definido por TOGAF para el desarrollo de una arquitectura empresarial que cumpla con las necesidades empresariales y de tecnología de la información de una organización** y proporciona un ciclo iterativo probado para crear arquitecturas resilientes y adaptables.

Video introductorio para la Fase Preliminar y Fase A

<https://youtu.be/Y9FYMGXQJ5I?si=a0boLXPXXviAgDT2>



### Alineación Estratégica Ciberseguridad

Conecta objetivos de negocio con capacidades tecnológicas, asegurando que cada decisión de seguridad impulse el crecimiento empresarial.



### Defensa en Profundidad

Implementa arquitecturas Zero Trust con múltiples capas de protección, desde el perímetro hasta el núcleo de datos.



### Gestión Inteligente

Optimiza la gestión de riesgos y cambios mediante procesos estructurados que anticipan amenazas emergentes.

### Colaboración Efectiva

Facilita la sinergia entre equipos de negocio y TI, creando un lenguaje común para la innovación segura.

# Fase Preliminar: Cimentando el Éxito



## Definición de Alcance



Establecimiento preciso de límites, recursos y expectativas para la arquitectura de seguridad



## Adaptación de TOGAF



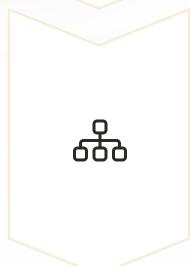
Personalización del marco para las necesidades específicas del sector fintech



## Mapeo de Stakeholders



Identificación y alineación de todos los actores clave en el ecosistema de seguridad

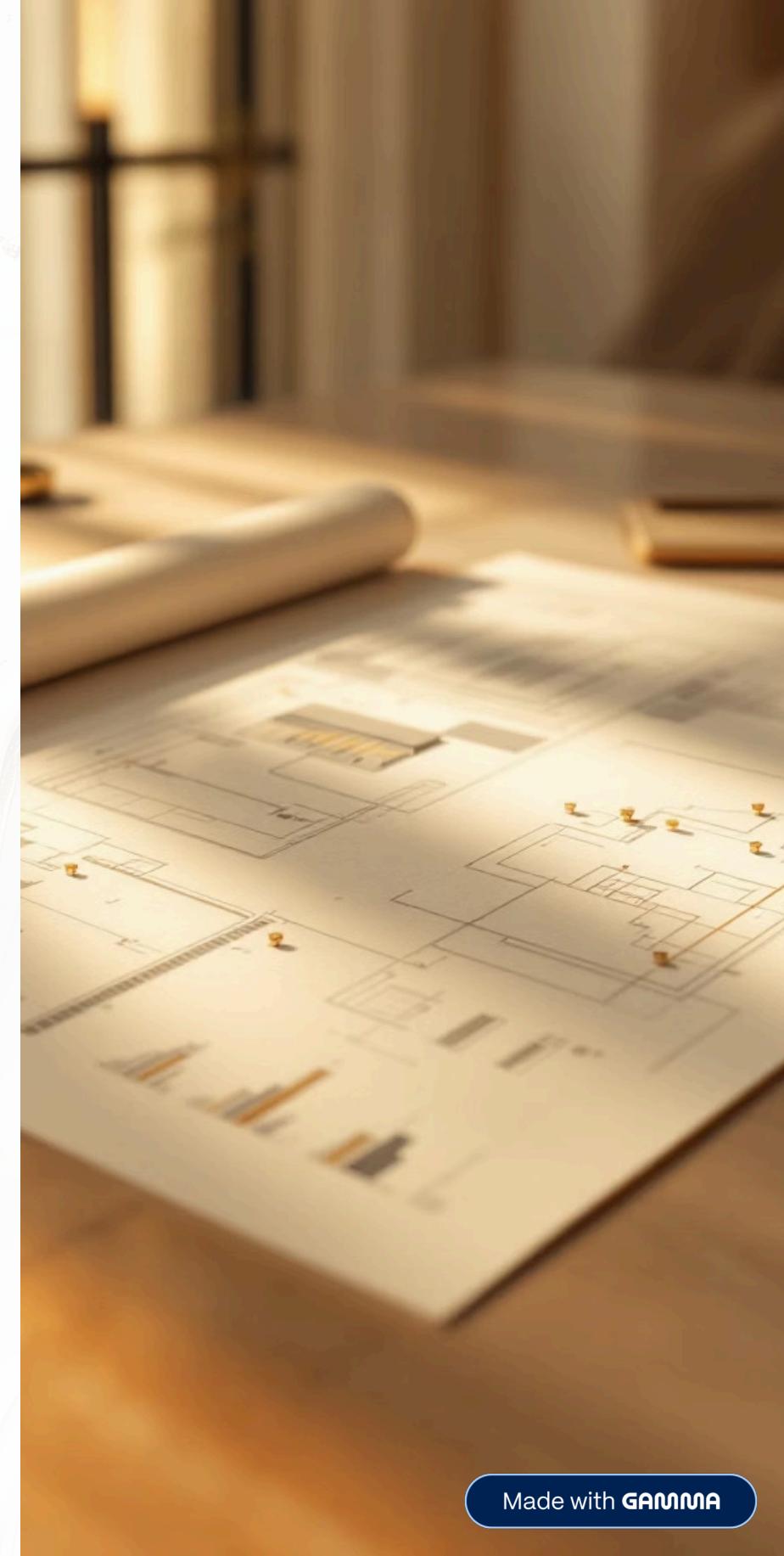


## Principios Arquitecturales



Establecimiento de directrices fundamentales que guiarán todas las decisiones futuras

**Entregables Clave:** Documento de Principios Arquitecturales • Mapa Detallado de Stakeholders • Plan de Trabajo Estratégico • Plan de Arquitectura



# Fase A: Construyendo la Visión del Futuro



## Objetivos Estratégicos

Identificación y alineación de metas de seguridad con la estrategia empresarial global



## Alcance Técnico

Definición precisa: Core bancario, infraestructura de nube híbrida y SOC avanzado



## Análisis de Amenazas

Mapeo comprensivo de riesgos emergentes y vectores de ataque específicos del sector

- ☐ **Resultado Principal:** Architecture Vision Document completo con diagramas conceptual de alto nivel, KPIs measurables y roadmap de implementación que se presenta después de la Fase A





# Banco Digital Seguro: Caso de Transformación

## Nuestra Misión

Democratizar la banca digital en Colombia, ofreciendo servicios financieros seguros, accesibles e innovadores para todos los segmentos de población.

## Visión de Seguridad

Convertirnos en la **Fintech más confiable de LATAM**, estableciendo nuevos estándares de seguridad y transparencia.

## Amenazas Priorizadas

Ransomware y Phishing.

## Ecosistema de Stakeholders

CEO • CISO • CIO • Superintendencia Financiera • Clientes • Auditores • Partners Tecnológicos

**99.99%**

**Disponibilidad**

Uptime garantizado 24/7

**0**

**Brechas de Datos**

Tolerancia cero a incidentes

**ISO 27001**

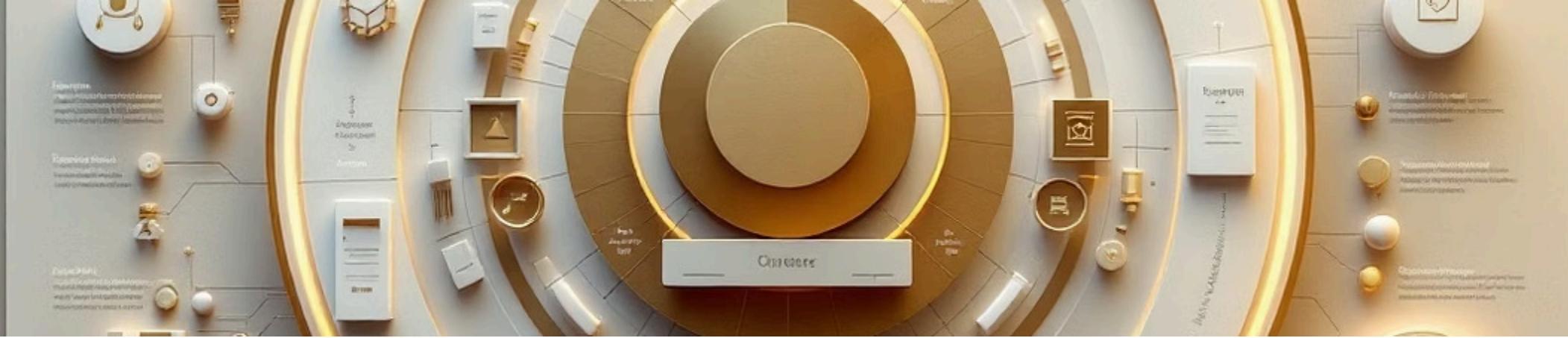
**Certificación**

Cumplimiento normativo completo

**KPI**

**Relevante**

MTTR < 30 minutos



# Arquitectura Visual y Roadmap Estratégico

## Fase 1: Diagnóstico

Evaluación completa del estado actual •  
Identificación de gaps críticos • Assessment  
de vulnerabilidades

## Fase 3: Hardening

Fortalecimiento de infraestructura •  
Implementación Zero Trust • Controles  
avanzados

1

2

3

4

## Fase 2: Quick Wins

Implementación de controles básicos •  
Mejoras inmediatas de seguridad • Training  
del equipo

## Fase 4: SOC & IA

Centro de operaciones 24/7 •  
Automatización inteligente • Respuesta  
predictiva

**Arquitectura de Alto Nivel:** Usuarios → Aplicaciones → Core Bancario → Nube Híbrida → SOC Inteligente

Con TOGAF como guía, hemos transformado la visión en realidad, creando una arquitectura de seguridad que no solo protege, sino que habilita la innovación continua en el ecosistema fintech.