

**CVDex**

# **AWS\_Architecture**

Finanzas SD – Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

November 10, 2025

## 1 AWS Architecture / Arquitectura AWS

### 1.1 EN: AWS Infrastructure Architecture

#### 1.1.1 Overview

The Finanzas SD system is built on AWS using serverless and managed services for scalability, security, and cost-effectiveness.

#### 1.1.2 Core Services

##### Compute & API Layer

- **AWS Lambda:** Serverless compute for all business logic
  - Pre-factura processing functions
  - Budget calculation functions
  - Document generation functions
- **Amazon API Gateway:** RESTful API endpoints with throttling and caching
  - /api/prefacturas - Pre-factura management
  - /api/budgets - Budget operations
  - /api/reports - Report generation

##### Data Layer

- **Amazon DynamoDB:** NoSQL database for high-performance data storage
  - prefacturas table - Pre-factura records
  - budgets table - Budget allocations
  - audit\_logs table - Audit trail
  - users table - User profiles and preferences
  - projects table - Project metadata
  - approvals table - Approval workflow state
  - notifications table - System notifications
  - documents table - Document metadata
  - settings table - System configuration

##### Storage & Content Delivery

- **Amazon S3:** Object storage for documents and static assets
  - Generated PDFs and CSV files
  - Uploaded attachments
  - Static web assets

- **Amazon CloudFront:** CDN for global content delivery
  - Cached API responses
  - Static asset delivery
  - Geographic distribution

## Security & Access Control

- **AWS Cognito:** User authentication and identity management
  - User pools for authentication
  - Multi-factor authentication (MFA) support
  - OAuth 2.0 / OpenID Connect integration
- **Amazon Verified Permissions (AVP):** Fine-grained authorization
  - Cedar policy engine
  - Role-based access control (RBAC)
  - Attribute-based access control (ABAC)
  - Policy store for centralized policy management

## Integration & Monitoring

- **AWS CloudWatch:** Monitoring, logging, and alerting
  - Application logs
  - Performance metrics
  - Custom dashboards
  - Alarm configuration
- **AWS X-Ray:** Distributed tracing for performance analysis
- **AWS EventBridge:** Event-driven architecture support

### 1.1.3 High Availability & Disaster Recovery

- Multi-AZ deployment for DynamoDB
- S3 cross-region replication for critical documents
- CloudFront edge locations for global availability
- Automated backups with point-in-time recovery

### 1.1.4 Security Best Practices

- Encryption at rest (S3, DynamoDB)
- Encryption in transit (TLS 1.2+)
- IAM least-privilege access policies

- VPC endpoints for private connectivity
  - AWS WAF for API protection
  - CloudTrail for comprehensive audit logging
- 

## 1.2 ES: Arquitectura de Infraestructura AWS

### 1.2.1 Descripción General

El sistema Finanzas SD está construido en AWS utilizando servicios sin servidor y administrados para escalabilidad, seguridad y rentabilidad.

### 1.2.2 Servicios Principales

#### Capa de Computación y API

- **AWS Lambda:** Computación sin servidor para toda la lógica de negocio
  - Funciones de procesamiento de pre-facturas
  - Funciones de cálculo de presupuesto
  - Funciones de generación de documentos
- **Amazon API Gateway:** Endpoints de API RESTful con limitación y caché

#### Capa de Datos

- **Amazon DynamoDB:** Base de datos NoSQL para almacenamiento de alto rendimiento
  - Tabla prefacturas - Registros de pre-facturas
  - Tabla budgets - Asignaciones de presupuesto
  - Tabla audit\_logs - Registro de auditoría
  - Tabla users - Perfiles de usuario y preferencias
  - Tabla projects - Metadatos de proyectos
  - Tabla approvals - Estado del flujo de trabajo de aprobación
  - Tabla notifications - Notificaciones del sistema
  - Tabla documents - Metadatos de documentos
  - Tabla settings - Configuración del sistema

#### Almacenamiento y Distribución de Contenido

- **Amazon S3:** Almacenamiento de objetos para documentos y activos estáticos
- **Amazon CloudFront:** CDN para entrega global de contenido

## Seguridad y Control de Acceso

- **AWS Cognito:** Autenticación de usuarios y gestión de identidad
- **Amazon Verified Permissions (AVP):** Autorización de grano fino
  - Motor de políticas Cedar
  - Control de acceso basado en roles (RBAC)
  - Control de acceso basado en atributos (ABAC)

## Integración y Monitoreo

- **AWS CloudWatch:** Monitoreo, registro y alertas
- **AWS X-Ray:** Rastreo distribuido para análisis de rendimiento
- **AWS EventBridge:** Soporte de arquitectura basada en eventos

### 1.2.3 Alta Disponibilidad y Recuperación ante Desastres

- Implementación Multi-AZ para DynamoDB
- Replicación entre regiones de S3 para documentos críticos
- Ubicaciones perimetrales de CloudFront para disponibilidad global
- Copias de seguridad automatizadas con recuperación a un punto en el tiempo

### 1.2.4 Mejores Prácticas de Seguridad

- Cifrado en reposo (S3, DynamoDB)
- Cifrado en tránsito (TLS 1.2+)
- Políticas de acceso IAM de mínimo privilegio
- Endpoints VPC para conectividad privada
- AWS WAF para protección de API
- CloudTrail para registro de auditoría exhaustivo

AWS Architecture Diagram