SMBCTEX-002 – Solution Configuration Document

Customer: Seguros Patria, S.A.
Project Code: IX-RD-PS-SegurosPatria-0 Migración infraestructura Seguros Patria
Version: 1.0
Date:
Prepared by: Intcomex Cloud
AWS Region: US East (N. Virginia)

Introduction

This document describes the configuration of the solution deployed for Seguros Patria on AWS. It outlines the key AWS services, software components, integrations, and system parameters necessary to support the solution in both production and development environments.

System Overview

The deployed solution includes components for compute, storage, networking, security, and monitoring, integrated to support Seguros Patria's insurance platform.

AWS Services and Configurations

Amazon EC2

- **OS:** Windows Server
- **Use Case:** Application hosting and IIS web services
- **Patching:** AWS Systems Manager Patch Manager (scan only; manual install)

Amazon RDS (SQL Server)

- **Engine:** Microsoft SQL Server
- **Deployment Mode:** Multi-AZ disabled (single AZ by client request)
- **Backups:** Daily snapshots via AWS Backup
- **Monitoring:** CloudWatch (performance metrics enabled)

AWS Directory Services

- **Use Case:** Replaces on-prem Active Directory
- **Authentication:** Secure directory-based access for domain-joined instances

Amazon FSx for Windows File Server

- **Purpose:** Shared file storage for user and app data

- **Configuration:** Automatically scales with demand

AWS Elastic Block Store (EBS)

- **Volume Types:** General Purpose SSD (gp2/gp3)
- **Backup:** EBS snapshot backups via AWS Backup

AWS Systems Manager

- **Modules Used:**
    - Patch Manager (for vulnerability scanning)
    - Session Manager (secure access)
    - Compliance Dashboard

Web & Networking Stack

Microsoft IIS

- **Purpose:** Hosts Seguros Patria's website
- **Integrated AWS Services:**
    - **AWS WAF:** Web Application Firewall to block malicious traffic
    - **AWS CloudFront:** CDN for performance
    - **AWS Application Load Balancer (ALB):** Balances traffic across EC2 instances
    - **Amazon Route 53:** DNS resolution for web assets

Amazon VPC

- **Configuration:** Custom VPC with public and private subnets
- **Security Groups:** Defined for each service role (Web, DB, AD, etc.)
- **NACLs:** Configured for subnet-level traffic control
- **Landing Zone:** Implemented to organize accounts, manage identity and governance

Security Configuration

IAM and Access Controls

- **Root Account:** MFA enabled
- **Users/Roles:** IAM policies enforce least privilege access
- **Temporary Credentials:** Configured for Partner access

Encryption

- **In Transit:** TLS enabled with Certificate Manager
- **At Rest:** Encrypted using AWS-managed KMS keys
- **Certificates:** Issued via ACM for internal and external endpoints

Monitoring and Logging

Amazon CloudWatch

- **Dashboards:** Custom for EC2, RDS, ALB
- **Log Groups:** IIS Logs, RDS Logs, System Event Logs
- **Alarms:** Configured for CPU > 90%, Disk Space, RAM

AWS CloudTrail

- **Function:** Audit trail of console and API activities
- **Storage:** Logs stored securely in S3

Backup and Disaster Recovery

AWS Backup

- **Services Covered:** RDS, EBS
- **Frequency:** Daily
- **Retention:** As per policy
- **Recovery Objectives:**
    - **RTO:** 2 hours
    - **RPO:** 24 hours

Deployment Configuration

Environment Structure

- **Production:** Fully deployed
- **Testing/Dev:** Not yet deployed, recommended as future phase

Code Deployment

- **Manual Process:** Current deployment through manual processes
- **DevOps Recommendation:** Adopt CI/CD pipeline (e.g., CodeDeploy + CodePipeline)

Operational Procedures

Runbooks

- Operational guides shared with client
- Includes:
    - Backup restore procedures
    - Patch update process
    - Infrastructure validation checklist

Training

- Training sessions delivered via Microsoft Teams
- Architecture diagram shared