Regional government digital agency

How a major public administration transformed its citizen-facing platform into a secure, resilient, and scalable digital gateway

aws PARTNER Premier Tier Services

When millions of citizens depend on your digital platform to access essential public services—from healthcare portals to electoral information—failure is not an option. A major regional government agency responsible for one of Europe's largest public digital platforms faced a critical challenge: how to ensure 24x7 availability, defend against increasingly sophisticated cyber threats, and maintain performance during massive traffic spikes driven by elections, emergencies, and viral institutional content. They turned to T-Systems for a comprehensive AWS Managed Services solution that would transform their cloud operations and set a new standard for public sector digital excellence.

2M+ monthly portal visits | **24x7** security monitoring | **35+** hospital portals managed

"The combination of continuous security monitoring, proactive threat protection, and structured cloud governance has fundamentally transformed how we deliver digital services to our citizens. T-Systems doesn't just operate our infrastructure-they help us build a platform worthy of the public's trust."

— Technology Director, Regional Government Digital Agency

The client

This regional government digital agency serves as the central technology authority for one of Europe's most populous regions. Responsible for the digital transformation of all regional ministries, the agency manages a vast portfolio of citizen-facing platforms that form the backbone of public service delivery.

The agency's, institutional web platform alone encompasses the official government portal, regional gazette, transparency and participation portals, elections portal, budget information systems, 35 hospital portals, museum and cultural venues, and dozens of sector-specific services—more than 10,000 active pages serving millions of citizens. Any degradation in availability, security, or performance directly impacts the delivery of essential public services and the institutional credibility of the regional government.

The challenge: Defending a high-value public target

Public sector digital platforms are attractive targets. The agency's portals face continuous exposure to cyberattacks—application-layer exploitation attempts, automated malicious traffic, and denial-of-service patterns—with threat intensity spiking dramatically during electoral processes, large-scale public announcements, and emergency situations.

"The challenge wasn't just keeping the lights on," explains the T-Systems engagement team. "It was building a defensive posture robust enough to protect a platform where a security breach or extended outage would make national headlines."

The multi-account AWS environment demanded enterprise-grade governance: consistent security policies across organizational units, preventive controls through service control policies, centralized logging for auditability, and continuous security posture monitoring. The platform also needed to absorb unpredictable traffic spikes—scaling elastically for elections while maintaining response times during viral content events—all while operating under strict public sector compliance requirements including Spain's National Security Framework (ENS).

T Systems

The solution: Security-first managed services

Since May 2025, T-Systems has operated the agency's AWS environment under a comprehensive managed services framework that integrates cloud consumption, specialized engineering, structured governance, and continuous security operations into a unified model designed for mission-critical public sector workloads.

Multi-account landing zone architecture

The foundation is a structured landing zone with differentiated organizational units providing centralized governance, security by design, and controlled scalability. Service control policies enforce preventive controls across all accounts. Centralized logging enables full traceability and audit compliance. The architecture supports the agency's cloud strategy for institutional portals while enabling secure onboarding of new workloads.

Advanced threat protection

A comprehensive AWS WAF v2 framework provides application-layer protection with managed and custom rule sets, dynamic tuning against emerging attack patterns, and progressive hardening following detected threats. AWS Security Hub consolidates security findings. Amazon GuardDuty delivers intelligent threat detection. AWS Config ensures continuous configuration compliance. Mandatory Multi-Factor Authentication (MFA) for all Identity and Access Management (AWS IAM) identities reduces credential compromise risk.

24x7 observability and incident response

Native AWS monitoring through Amazon CloudWatch provides continuous supervision across Content Delivery Network (CDN) performance, serverless functions, and traffic patterns. Custom dashboards deliver real-time platform health visibility with thresholds calibrated for high-load events such as elections. Structured incident management covers the full lifecycle from detection through resolution, with continuous improvement cycles that harden defenses after each security event.

Public sector FinOps

For a publicly-funded institution, cost predictability is essential. AWS Budgets and cost anomaly detection provide early warning of spending deviations, with enhanced monitoring during high-demand periods. Continuous consumption analysis identifies optimization opportunities while ensuring the platform can scale when citizens need it the most.

The results: A platform citizens can trust

Strengthened security posture:

The comprehensive protection framework has significantly reduced attack surface exposure, with continuous Web Application Firewall (AWS WAF) hardening improving resilience against evolving threats.

Enterprise-grade resilience:

Multi-Availability Zone (Multi-AZ) architecture and AWS-managed services provide structural fault tolerance. The platform absorbs traffic spikes during elections and emergencies while maintaining performance.

Operational maturity:

Structured governance, defined IT Service Management (ITSM) processes, and well-architected alignment have transformed cloud operations from reactive to proactive.

Reduced institutional risk:

With continuous monitoring and rapid incident response, the risk of headline-making outages or breaches has been qualitatively reduced.

Looking forward: Full Cloud transformation

The partnership continues to evolve. The agency is progressively migrating on-premises portals to Amazon EKS, consolidating towards a fully AWS-hosted architecture throughout 2026. T-Systems provides architectural guidance, migration support, and container platform expertise—ensuring this mission-critical institutional platform remains secure, resilient, and ready to serve citizens for years to come.

AWS Services & Technologies Managed

- Amazon CloudFront · AWS WAF v2 · AWS Lambda · Amazon CloudWatch · AWS MediaLive · AWS Organizations
- AWS Security Hub · Amazon GuardDuty · AWS Config · AWS Budgets · AWS Cost Anomaly Detection
- Elastic Kubernetes Service (Amazon EKS) (in progress)

Industry Public sector & government **Location** Spain

Contact
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
E-Mail: AWS-Info@t-systems.com
Website: www.t-systems.com

Published by
T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main
Germany

T Systems