Telefónica Tech

Application Resiliency

Continuous protection for your applications, from development to execution.

What is it?

It is the ability of an application to **remain operational in the event of technical failures or cyberattacks**, it is based on four pillars:

- Prevention
- Protection
- Identification
- Remediation

Why is it key for your business?

- **Reduces downtime**
- **Improves user experience and ensures operational continuity**
- **Minimizes economic and reputational impact in the event of interruptions or attacks**
- **Strengthens security against threats that affect both applications and the underlying infrastructure**

Current context

+97.000

+Over 97,000 Cyber Security incidents managed by INCIBE in 2024 in Spain.

55%

55 % of cloud breaches were due to human error or incorrect configurations (*Thales Group*).

40%

Only 40% of companies effectively prioritize vulnerabilities, meaning that **60% face difficulties** in this area (*Tenable*).

Telefónica Tech's approach is based on four pillars

Pillar	Purpose	Key value
Prevention	Early-stage analysis of development and CI/CD processes.	Reduces attack surface and errors from the design stage.
Protection	WAF, defense against DDoS, bots, APIs, microsegmentation, and CNAPP.	Real-time blocking, increased availability.
Identification	Continuous monitoring and detection of anomalies and vulnerabilities.	Anticipation and reduction of exposure time.
Remediation	Automation of responses and integration with operational and business processes.	Rapid containment and improved recovery capability.

Application resiliency across the lifecycle

Phase 1 **Planning and design**	Resilient-by-design architectures.	Threat modeling and definition of RTO/RPO objectives.	Microsegmentation to contain breaches from the design stage.
Phase 2 **Secure Development and DevSecOps**	Security integrated into pipelines.	Continuous code and infrastructure analysis.	Early validation with load testing and vulnerability scans.
Phase 3 **Protection and operation**	Access controls, specialized firewalls, and logical segmentation.	Auto-scaling, balancing, and automated recovery.	Real-time monitoring to detect anomalies.
Phase 4 **Response and continuous improvement**	Automated response through security orchestration.	Structured review of incidents and application of lessons learned.	Continuous reinforcement with AI, managed detection, and threat intelligence sources.

Challenges it solves

- **Attacks on applications and APIs**
- **Lateral expansion of ransomware**
- **Publication without failure testing**
- **Slow recovery from incidents**
- **Lack of visibility**

Telefónica Tech's differentiated services

- **Web Application Defense (WAD)**
  24/7 defense against OWASP threats, malicious bots, exposed APIs, and denial-of-service (DDoS) attacks.
- **Microsegmentation**
  Granular control of traffic between applications, workloads, and users, both on-premises and in the cloud.
- **Cloud Security**
  Protecting cloud environments with advanced threat detection, automated response, and continuous visibility.
- **Vulnerability Exposure**
  Continuous assessment service that identifies and prioritizes vulnerabilities in applications and systems.

Leadership and expertise at the service of your company

- Personalized advice based on risks and business objectives.
- Proactive monitoring and response with AI and application security experts.
- Specialized support in technologies with manufacturer certification.
- Security and policy management by a leading team, improving efficiency and security posture.

Benefits for your business

- Reduction of interruptions in critical services.
- Improved operational efficiency.
- Optimization of the digital experience.
- Lower costs due to failures and attacks.
- Greater protection against human error and advanced threats.