SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

República del Perú

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

The DFS Security Lab Journey

From technical assistance to supervisory practice in Peru

Lesley Ortega
Technology Risk Supervision Department
Risk Management Unit
September 2026

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Agenda

1 **Evolution of the DFS Security Lab**

How did the DFS Security Lab evolve over time?

2 **Practical Insights from Mobile Security Testing in Peru**

What have we learned from testing mobile applications?

3 **Supervisory Impact and Future Directions**

How are testing results shaping supervisory activities and future initiatives?

1

Evolution of the DFS Security Lab

SBS's Mandate in the Digital Era

SBS Peru

Regulator and supervisor of Peru's financial, insurance and private pension systems.

Core mandate: • financial stability • protection of financial users

WHY TECHNICAL SUPERVISION MATTERS?

1 Financial Services Go Digital

- More financial services delivered digitally
- Growth of mobile applications

2 Greater Adoption and Usage

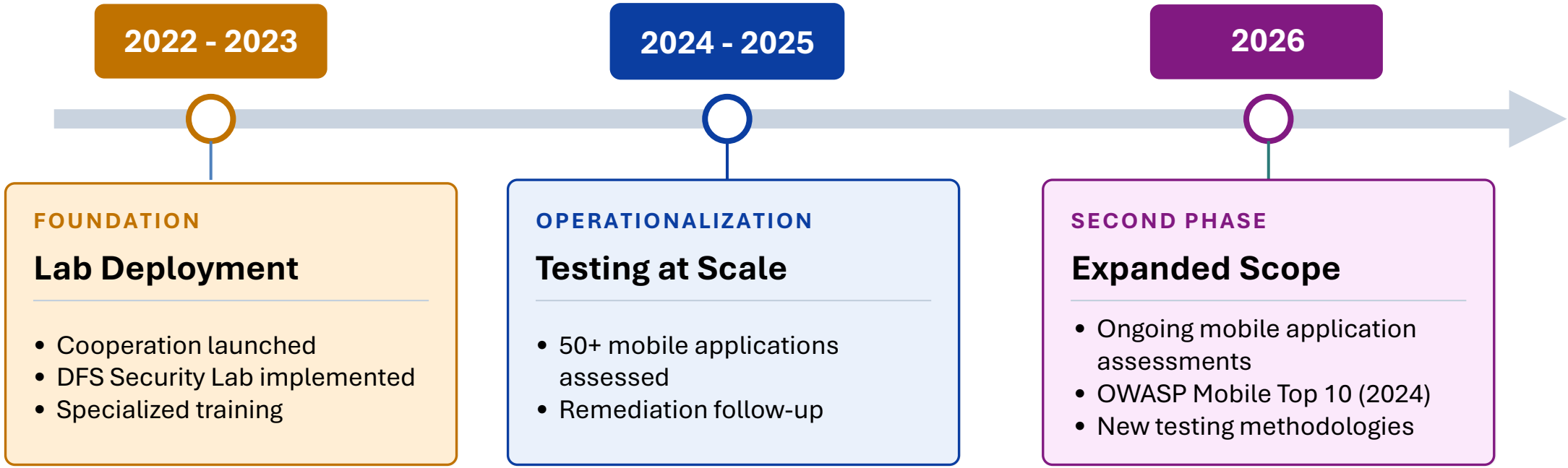
- More users and transactions
- Greater connectivity and mobile usage

3 Supervisory Challenge

- Security and resilience of digital services
- Emerging cyber and fraud risks

As digital financial services expand, SBS requires technical evidence to support risk-based supervision and user protection.

A Multi-Year Journey with ITU



CONTINUOUS ITU COOPERATION | Knowledge transfer • Security best practices • Case-specific technical support

A sustained partnership, continuously adapted to evolving threats and supervisory needs.

Two Iterations, Continuous Improvement

	FIRST PHASE	SECOND PHASE
FOCUS	Build foundational testing capabilities	Expand and mature supervisory testing
FRAMEWORK	OWASP Mobile Top 10 (2016)	OWASP Mobile Top 10 (2024)
SCOPE	USSD, STK, Android and iOS	Android and iOS applications
TESTING MODEL	Baseline assessments and initial test cases	Enhanced techniques and updated test cases
SUPERVISORY VALUE	50+ applications assessed Initial remediation programs	Ongoing assessments Stronger supervisory integration

EVOLVING WITH THE DIGITAL FINANCIAL ECOSYSTEM

Continuous assessments supported by updated standards and testing methodologies

Practical Insights from Mobile Security Testing in Peru

Practical testing experience

ANDROID — Operational testing capability

COMMON ASSESSMENT ACTIVITIES

1. Authentication and Authorization
2. Input Validation
3. Secure communications
4. Binary protections
5. Security misconfiguration
6. Data protection and cryptography

iOS — Knowledge transfer in progress

COMMON ASSESSMENT ACTIVITIES

1. Local Authentication
2. Universal Links & URL Schemes
3. Secure communications
4. Binary protections
5. Security misconfiguration
6. Data protection and cryptography

Current stage: methodology transfer and guided testing

TESTING SCOPE

- ✓ **Mobile banking applications**
- ✓ **Remediation validation**
- ✓ **Licensing applicants**

The apps are becoming more challenging

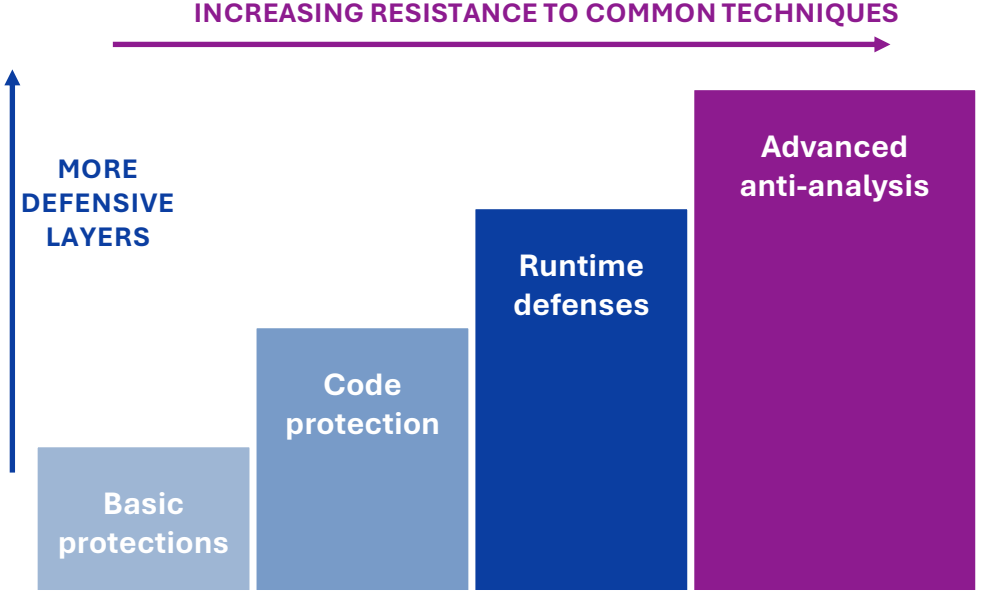
EARLIER ASSESSMENTS

Lower testing barriers

- Limited defensive controls
- Basic application protections
- Standard bypass techniques often sufficient

CURRENT ASSESSMENTS

More layers. Stronger implementations.



Traditional controls are becoming harder to bypass, while new defensive layers continue to emerge

IMPLICATION FOR THE LAB

More research-intensive assessments

1. Custom controls require application-specific analysis
2. Research may take longer than test execution
3. Continuous capability development is required

KEY INSIGHT | More layers + stronger implementations = more challenging assessments

A heterogeneous security landscape

MATURITY SPECTRUM

DEVELOPING MATURITY

Institutions at an earlier stage of adoption

1. Uneven adoption of application security controls
2. Recurring weaknesses observed more frequently
3. Secure development practices still evolving

HIGHER MATURITY

Institutions with more mature practices

1. More robust and layered application protections
2. Fewer critical findings in tested applications
3. Secure development practices more embedded

SUPERVISORY LENS

The objective is not to compare institutions, but to understand different maturity levels and support continuous improvement.

Recurring weaknesses and emerging challenges

DATA PROTECTION

Sensitive information exposure

APPLICATION HARDENING

Insufficient reverse engineering protection

SECURE COMMUNICATIONS

Weak or inconsistent configurations

DEVICE INTEGRITY

Inconsistent root / jailbreak controls

EMERGING CHALLENGES

1. More complex application architectures
2. New anti-analysis mechanisms
3. Greater runtime protection complexity

3

Supervisory Impact and Future Directions

Impact of the Supervisory Model

PREVIOUS MODEL

Separate supervisory communication

1. Testing activity
2. Technical report
3. Ad-hoc communication

EVOLUTION

CURRENT MODEL

Mobile app testing embedded in the inspection cycle

1 SUPERVISORY INSPECTION

The inspection may include:

- **Mobile application** security testing
- **Digital channel** authentication assessment
- **Secure development** practices review

ITU Recommendations

2 Inspection Findings & Recommend ations

3 Follow-up Actions

ITU guidance translated into supervisory recommendations.

App findings integrated into supervisory follow-up.

Future Directions

1

2

3

NEAR TERM

Consolidate

- Complete adoption of OWASP Mobile Top 10 2024.
- Complete security assessments of all mobile applications.

MEDIUM TERM

Institutionalize

- Expand mobile security testing knowledge across the entire supervision team.
- Integrate the methodology into supervisory activities.

LONG TERM

Promote

- Strengthen technical cooperation and knowledge sharing.

Benefits and achievements

Improved **visibility into security weaknesses** affecting DFS mobile applications.

Technical testing capabilities incorporated into supervisory activities

Stronger supervisory capacity to address emerging digital security risks.

Contribution to **risk-based** technology supervision

Successful collaboration with ITU in building technical capacity

Thanks