

República del Perú



ITU Webinar: Best Practices for Securing Mobile Payment Applications (Part 2)

# The SBS Peru Experience with the ITU DFS Security Lab, enhancing Mobile Payment Application Security.

Magno Condori Information Systems and Technology Supervision Department Risk Management Unit April 28, 2025

### Agenda



### **Introduction - SBS Peru's Mandate in the Digital Era**

- SBS: Regulator and supervisor of the financial, insurance, and private pension systems in Peru. It does not include security market and monetary policy.
- Core Mandate:
  - Promoting the stability of the financial system.
  - Protecting the interests of financial users.

#### **Digital Transformation**

**Rapid growth** of Digital Financial Services (DFS), especially mobile payments, in Peru.

#### New Challenges

Ensuring the **security and resilience** of these digital services is crucial for both **stability and user protection.** 

#### **Focus Today**

Our experience in regulating and supervising mobile payment security, highlighting the role of the **ITU DFS Security Lab.** 

### The Evolving Landscape of Mobile Payment Security

## Landscape

Mobile payments offer convenience but also present new security risks.

**Threat actors** constantly target mobile applications to compromise data and funds.

Importance of robust **security measures** throughout the **application lifecycle**.

• -----

## Technical Standard

OWASP Mobile Application Security Testing Guide (MASTG)

OWASP MASVS (Mobile Application Security Verification Standard)



## Methodology

ITU-T Recommendation X.1150 (Security assurance framework for DFS)

#### **SBS's Approach: Regulation and Supervision**

### Regulation

Adapting our regulatory framework to address digital and cybersecurity risks in DFS.

#### Requirements

Establishing clear security requirements for financial institutions offering mobile payment services.

### **Supervision**

Supervisory efforts focused on ensuring compliance with these regulations.

#### Moving towards more proactive and technically-driven supervision.

### **Strengthening Technical Supervision Capabilities**

Traditional supervision methods needed enhancement to effectively assess the technical security of mobile applications.

Recognizing the need for hands-on testing and in-depth analysis of application security.

**Objective:** Gain a deeper understanding of specific security challenges in mobile payment apps.

### Implementing the ITU-Supported DFS Security Lab



### The Lab in Action: Security Testing Methodology



Utilizing the lab for systematic **security assessments** of mobile payment applications used by regulated entities.

Employing testing **methodologies aligned** with best practices (e.g., based on OWASP MASTG).



Examples of testing: insecure data storage, insecure communication, insecure authentication, code tampering, reverse engineering, etc.



Performing static and dynamic analysis of the applications, particularly focusing on Android and iOS applications.

## **Key Findings: Identifying Vulnerabilities**



Lab testing has allowed us to **identify specific vulnerabilities** present in mobile payment applications operating in Peru.



Types of **vulnerabilities** observed (e.g., weaknesses in encryption, improper handling of sensitive data, insufficient authentication checks).



These findings provide **concrete evidence** for supervisory actions and subsequent treatment by financial institutions.

### Impact of the Lab: Enhanced Supervision and Knowledge

The lab **provides a more technical and evidencebased foundation** for our supervision of mobile application security.

**Increased Supervisory** 

Depth

Our supervisory team has gained valuable hands-on experience and a deeper understanding of the specific technical security challenges in mobile apps.

**Team Familiarization** 

Ability to proactively identify **potential systemic vulnerabilities** that could affect multiple applications.

**Proactive Identification** 

### **Ensuring Remediation: Vulnerability Treatment**



#### **Benefits and Achievements**

Improved **security level** of mobile payment applications in the Peruvian market. Better-equipped supervisory authority to address emerging digital security threats. Increased **confidence** in digital financial services among users, supporting financial inclusion.

Contribution to the overall **stability and integrity** of the financial system. Successful collaboration with the ITU in building technical capacity.

### **Conclusion and Key Takeaways**

- Securing mobile payment applications is an ongoing and critical effort for regulators.
- A combination of clear regulation, effective supervision, and technical testing capabilities is essential.
- The ITU-supported DFS Security Lab has been a transformative initiative for SBS Peru's IT supervisory approach.
- We remain committed to leveraging technology and collaboration to ensure a secure digital financial ecosystem for all users.



The Superintendency of Banking, Insurance, and AFP is the owner of this document. No part of its content may be reproduced, stored, duplicated, copied, or distributed in any form or by any means without the express prior consent of the Superintendency of Banking, Insurance, and AFP.