INE’s Strategy on Cybersecurity in 2018

IFES, U.S.A. November, 2018.

Instituto Nacional Electoral

Background

In Mexico, the so called “fall of the system” on 1988 meant, for some, the point of departure of the transition to democracy and the main incentive to never spare resources of any kind on ICT security.

Avoiding suspiciousness due to failure of ICT systems and averting opacity of procedures, left a lasting mark on Mexican political culture.

Hence, since the foundation of IFE y now with INE, we have given special attention to our ICT systems.

Main forseen risks

Having to face the largest electoral process in the history of Mexico, we identified the following 6 risks that helped us guide our protection efforts in 2018:

1. **Service denial** (artificial intense traffic to hinder response)
2. **Continuity of processes** (prevention against natural phenomena)
3. **Hacking attempts to institutional web sites**
4. **Internally undertaken attacks**
5. **Fake News**
6. **Malware attacks** (attempts to hit computing equipment through viruses or computer worms)

Protection Strategy

To deal with these risks we concibed and followed a strategy in two tiers:

1. Bringing together *expertise* and creating synergies with other institutions and organisations (academia, Facebook, Google, Twitter, etc.).

2. “Translating” the experiences of the participants in the first tier into technical innovations, in orden to adapt, modernize and protect our systems from the identified attack risks.

Protection Strategy

(1) Participation of Civil Society and Academia

This is carried out through Technical Committees (PREP, Quick Counting) composed by independent experts:

- Following up of ICT projects and issuing of recommendations.
- IN HOUSE development of the sensitive electoral programs (PREP, QC, etc.).
- **Auditting undertaken by reknowned academic institutions** (UNAM, IPN, Monterrey Technology Institute) with focus on aspcts such as **source code, security and functionins of the systems**.
- Testing of the systems through simulated attacks.

Protection Strategy

(2) Key Alliances against Fake News: FB, Google & Twitter

To counteract disinformation we signed collaboration agreements with leader social network firms (**Facebook, Google y Twitter) in order to address and fight disinformation with truthful and verifiable information**.

- **We are committed to information, not censorship** regarding the Electoral Process.
- We are committed to proactive explanation to avoid explaining as damage control.
- Therefore, the 2018 Election what the most explained in Mexican history, in order to **counteract fake news**.

Protection Strategy

(3) Scheme of Disseminating Partners of the PREP

To inform the preliminary results of the elections we had a network of **official disseminating partners**.

- **This network allowed to diversify risks**: the eventual failure of or attack to a single disseminating partner does not jeopardize the publishing of the preliminary electoral results.

Protection Strategy

(4) Cloud Migration of ICT

The ICT services with the greatest demand of computing resources were hosted in the cloud.

- **This allowed to strenghten the infrastructure** in the case of attacks of service denial and physical disasters, and increases the capacity to respond to large ammounts of demand in a timely manner.

- Increasing of the security levels with our software providers (Microsoft, Oracle, etc.)

Protection Strategy

(5) Strenghtening of Quality and Security Processes

During **every single phase of the implementation** of the systems we **include security measures**.

- We undertake **tests, exercises and simulations.**
- **Contractig the services of the most qualificated ITC security companies, permanently, but particularly during electoral phase.**
- **Improving continuity of operation process schemes during elections.**

Protection Strategy

(6) Certification of Technical Processes

An authorized officer –a public notary– accompanies the techincal team during the following stages:

- **Prior to the starting of operations:** s/he may certify that **the system which is about to start operations corresponds to the one being auditted** and that the **data bases are blanck**.

PORQUE MI PAÍS ME IMPORTA

INE
Instituto Nacional Electoral