Adaptive Cybersecurity Strategy for the Payment Methods Ecosystem in Latin America

PCI SSC North America Community Meeting

PCI Security Standards Council

Valther Galván

CISSP, ISA, PCIP, ISO/IEC 27001 Senior Lead Implementer
Chief Information Security Officer, PROSA

PROSA

PCI Security Standards Council®

Agenda

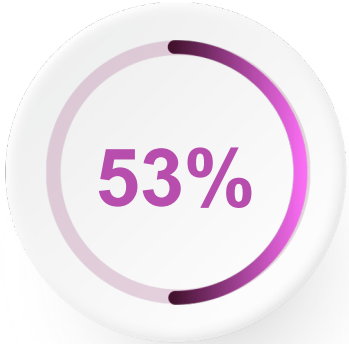
- Global Cybersecurity landscape
- Most relevant cyberattacks in LATAM
- Cybersecurity challenges for LATAM
- Cybersecurity in Latin America
- How do Latin Americans make their payments?
- Threats to the payment methods sector
- Adaptive Cybersecurity Strategy

Global Cybersecurity Landscape

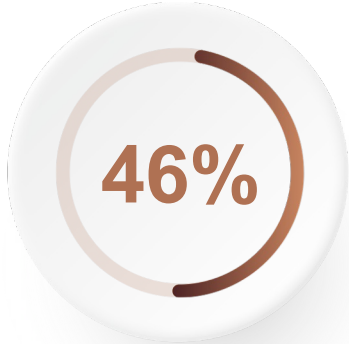
Cyberattacks on potential critical infrastructure are among the main risks for 2024 with the greatest impact on a global scale.

Cyber threats are constantly evolving, increasing in intensity and complexity.

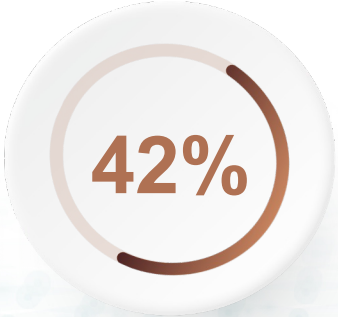
1st
Extreme weather



2nd
AI-generated misinformation



3rd
Societal and political polarization



4th
Cost-of-living crisis

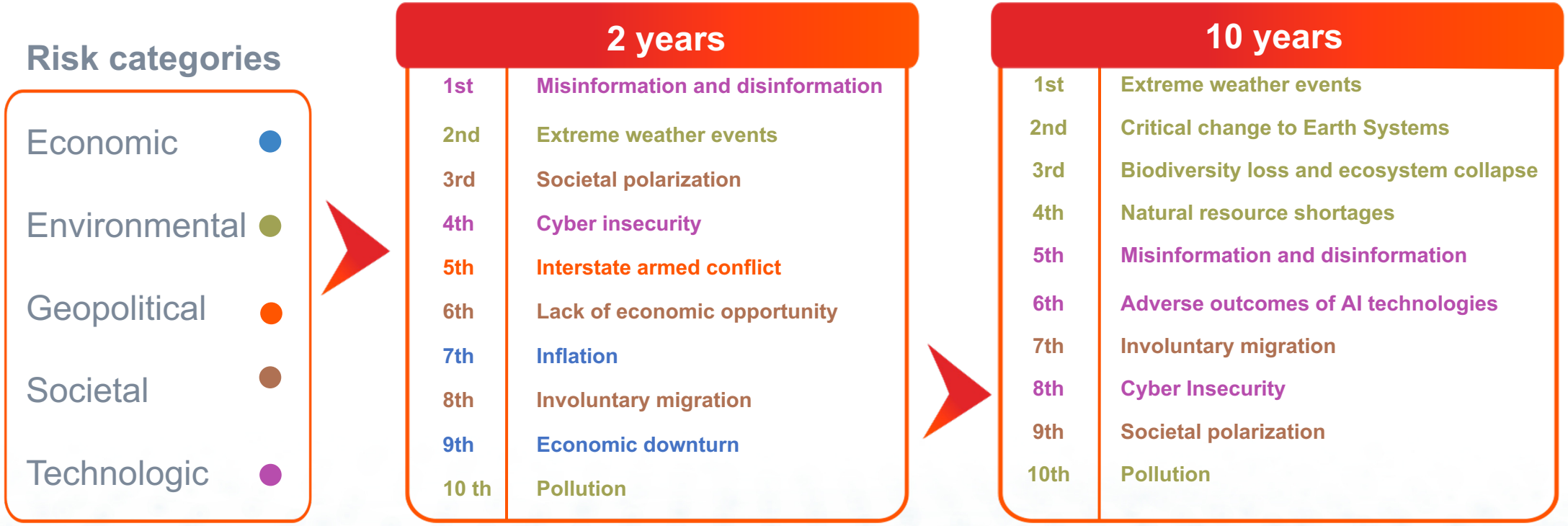
5th
Cyberattacks

Source: World Economic Forum Global Risks Perception Survey 2023-2024.

PCI Security Standards Council®

Global Cybersecurity Landscape

Information assets are companies' most valuable assets. Companies can only operate now or in the future with them.



Source: World Economic Forum Global Risks Perception Survey 2023-2024.

PCI Security Standards Council®

Most Relevant Cyberattacks in LATAM

Chronology of the most relevant cyberattacks in Latin America in the last ten years.

Operation Iceberg in to Brazil
2014

Attacks on Brazil Banking Systems
2014

Attacks on Critical Infrastructure in Mexico
2015

Attack on the Mexican Financial System
2018

Ransomware against Argentine banks
2019

Ransomware attack on US POS
2023

2017
Ransomware attacks on Latin America

2018
Attack on Chilean Banking

2019
Attacks on Critical Infrastructure in Venezuela

2020
Brazil cyberattacks on banks

2022
Cyberattack on Costa Rica Institutions

2024
Point-of-Sale Malware Campaigns

PCI Security Standards Council®

Most Relevant Cyberattacks in LATAM

Digital skimming attacks

- In digital skimming attacks, threat actors deploy malicious code onto merchant websites targeting checkout pages in attempts to harvest payment account data entered by consumers, such as primary account number (PAN), card verification value (CVV2), expiration date, and personal identifiable information (PII).

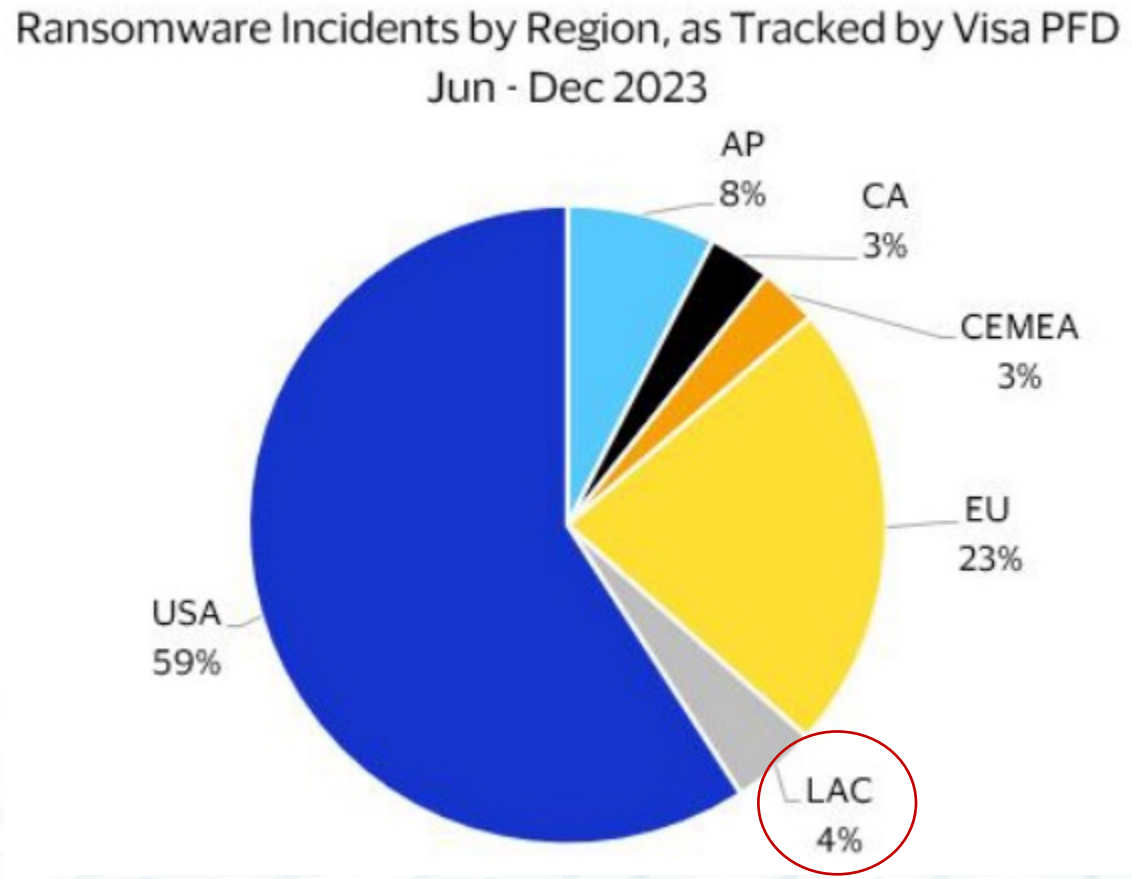
- In this attack, the threat actors gained initial access to the victim's systems through a public-facing management PHP file with a misconfiguration vulnerability allowing the threat actors to conduct SQL injection attacks against this file.

Source: Visa Payment Fraud Disruption
Biannual Threats Report December 2023

PCI Security Standards Council

Most Relevant Cyberattacks in LATAM

Ransomware increased 131% in total incidents tracked in 2023 vs 2022



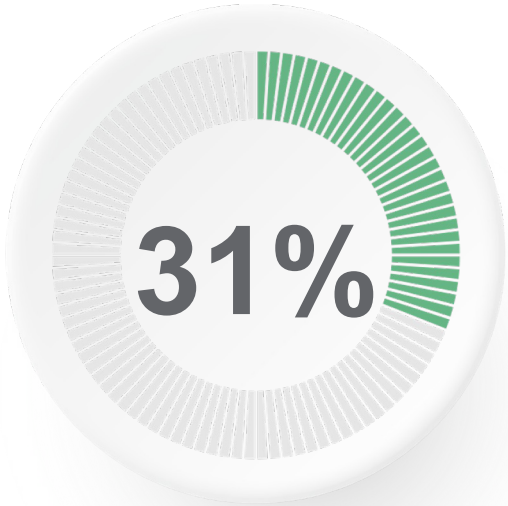
- Ransomware and data breach incidents involving data exfiltration remain prevalent and are an increasing threat across the payments ecosystem.
- Visa identified North America as the region most affected by ransomware and data breach incidents impacting the payments ecosystem.

Source: Visa Payment Fraud Disruption Biannual Threats Report December 2023

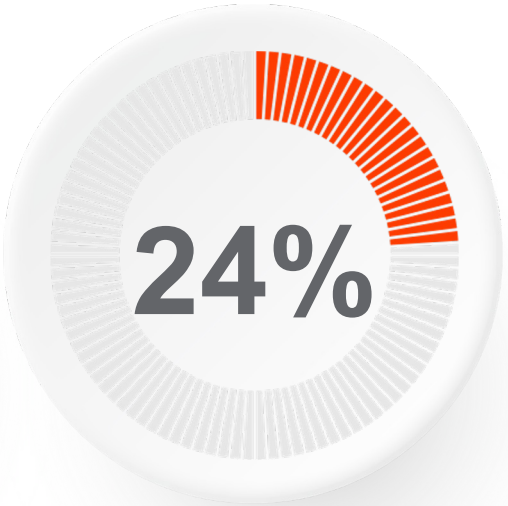
PCI Security Standards Council

Cybersecurity Challenges for LATAM

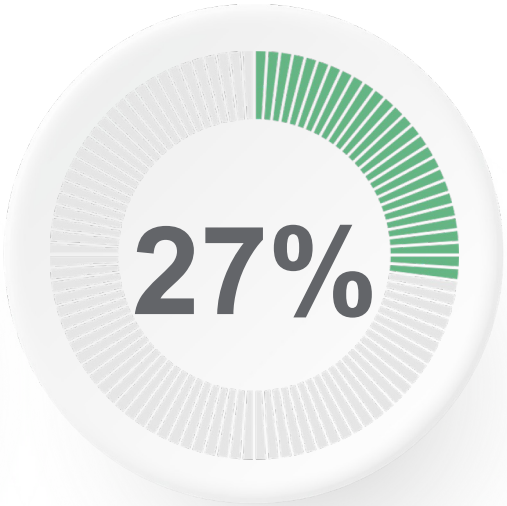
Social engineering or phishing is the cyberattack that increased the most in Latin America due to the pandemic.



Companies surveyed in Latin America have perceived increased cyber attacks since the pandemic, with the banking industry being the most affected.



Companies increased their cybersecurity budget and 26% in data protection as a result of the pandemic, and only 17% of organizations have cyber risk insurance.



Companies that implemented remote work, the workforce works exclusively with the organization's devices.

Social engineering:

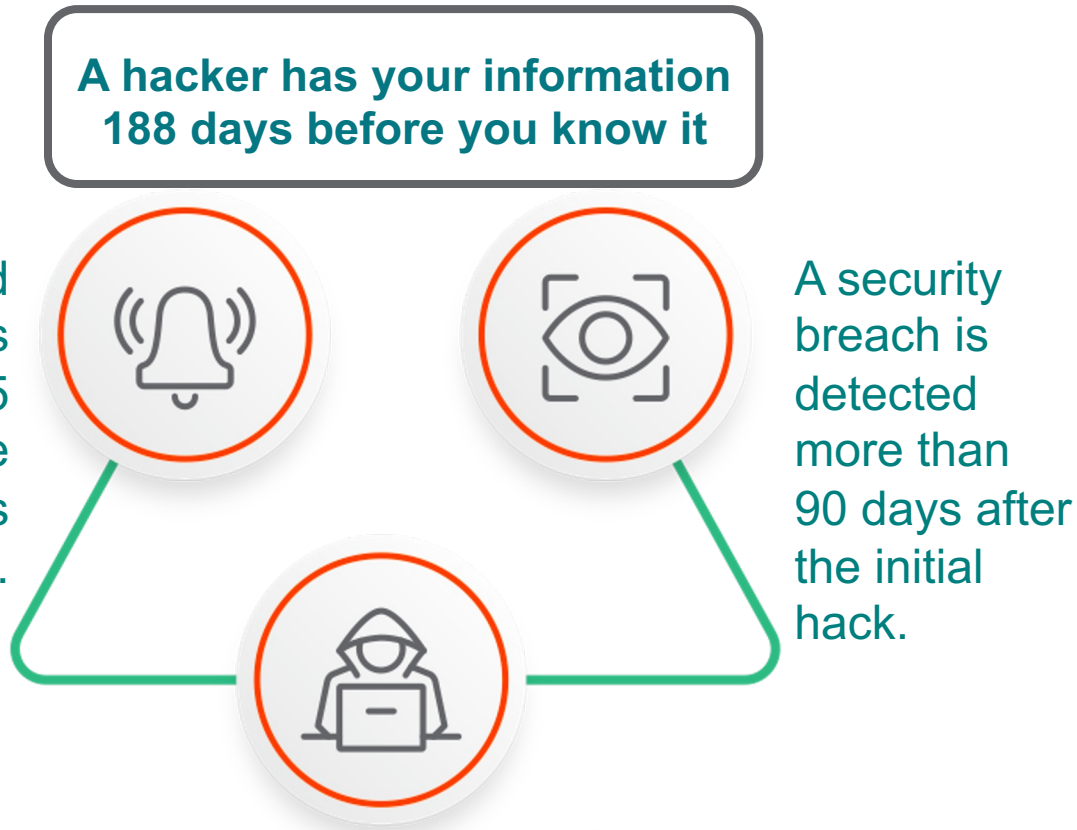
The intelligent manipulation of people's natural tendency to trust.

Source: News Center Microsoft Latinoamérica, Marsh y Microsoft: Report.

PCI Security Standards Council®

Cybersecurity Challenges for LATAM

- Constant evolution of threats
- Complexity of systems and technologies
- Shortage of specialized talent
- Regulatory and compliance changes
- Supply chain risk management
- Lack of safety awareness and culture



Source: Study of cyber risk management in the Latin American financial sector 2023, Marsh

PCI Security Standards Council

Cybersecurity in Latin America

A cybersecurity strategy is, therefore, an ongoing and complex effort.

- As of the beginning of 2020, only 12 countries had approved a national cybersecurity strategy (which can be deemed an accomplishment, considering that only five countries had a strategy since 2016).
- Moreover, only 10 countries established a centralized government entity to manage national cybersecurity.

Source: CYBERSECURITY RISKS, PROGRESS, AND THE WAY FORWARD IN LATIN AMERICA AND THE CARIBBEAN, 2020 Cybersecurity Report

PCI Security Standards Council

How Do Latin Americans Make Their Payments?

Mastercard reveals the preferences behind the payment methods of choice in Latin America and the Caribbean.

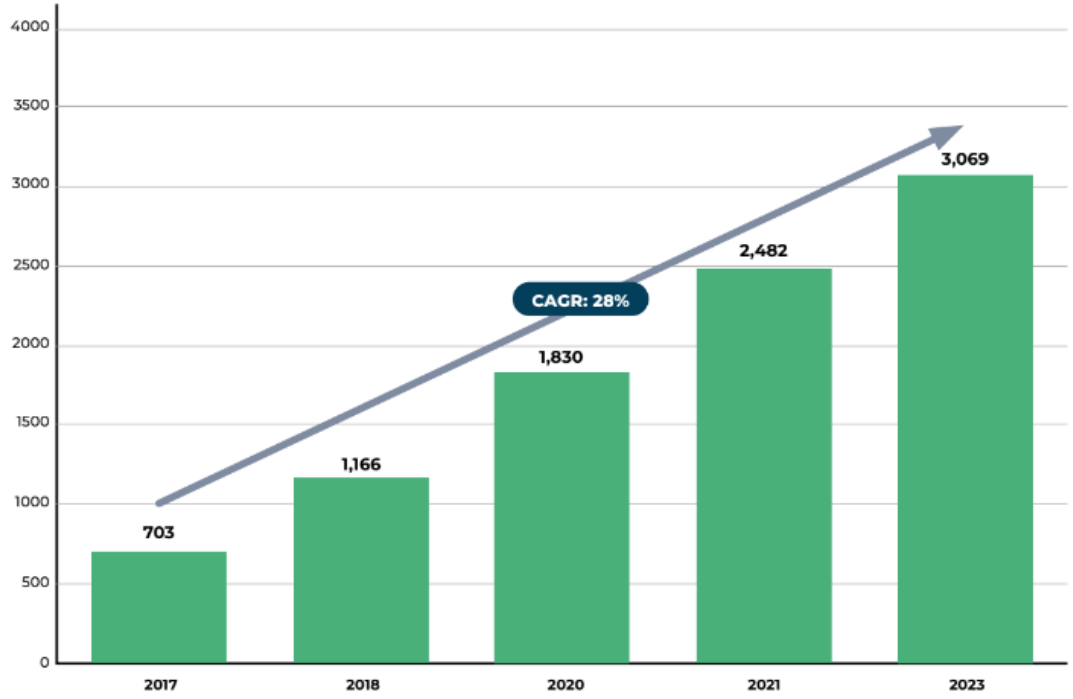
- Trust in cards remains despite new digital payment methods. **77% of the consumers have used electronic payments**, with credit and debit being the most utilized online and in-store payment instruments.
- Additionally, debit has been highlighted as the most important digital payment method, used by **63% of consumers**.
- **Protection from fraud** is the main factor influencing consumer behavior when choosing a payment method.

Source: Master Card Reference

PCI Security Standards Council

How Do Latin Americans Make Their Payments?

The Fintech ecosystem registered a growth of more than 340% in the number of technological finance startups created in the last six years, going from 703 companies in 18 countries in 2017 to 3,069 in 26 countries in 2023.



- ✓ Brazil has the highest % of fintech startups, with 24% of the total. **Mexico follows with 20%**, Colombia with 13%, and Argentina and Chile with 10% each.
- ✓ In the realm of cybersecurity, **78.74% of the companies** surveyed are not only aware of the threat posed by cybersecurity risks but are also actively taking, or planning to take, measures to protect themselves, whether through implemented security frameworks, insurance, or security strategies.

Source: Fourth report of the Fintech series in Latin America and the Caribbean., 20 Junio 2024, BID Inform

PCI Security Standards Council®

Threats to the Payment Methods Sector

The structure of the card payment market is configured in LATAM by incorporating new card payment networks.

Financial fraud in Mexico increased 10.4% since first half of 2022

According to CONDUSEF, 59% correspond to cyber fraud

CONDUSEF

17.5 million card details for sale in the black markets

Credit card details They are sold on the **black market.**

SOC RADAR

Ransomware attacks every 11s

Extortion demands have increased by 300% in a single year.

Forrester Predictions

Cybersecurity more strategic

By 2025, 40% of companies will have a cybersecurity committee

Gartner Board of Directors Survey

- USD 7 is the cost of a Mexican credit or debit card offered on the dark web, according to NordVPN.

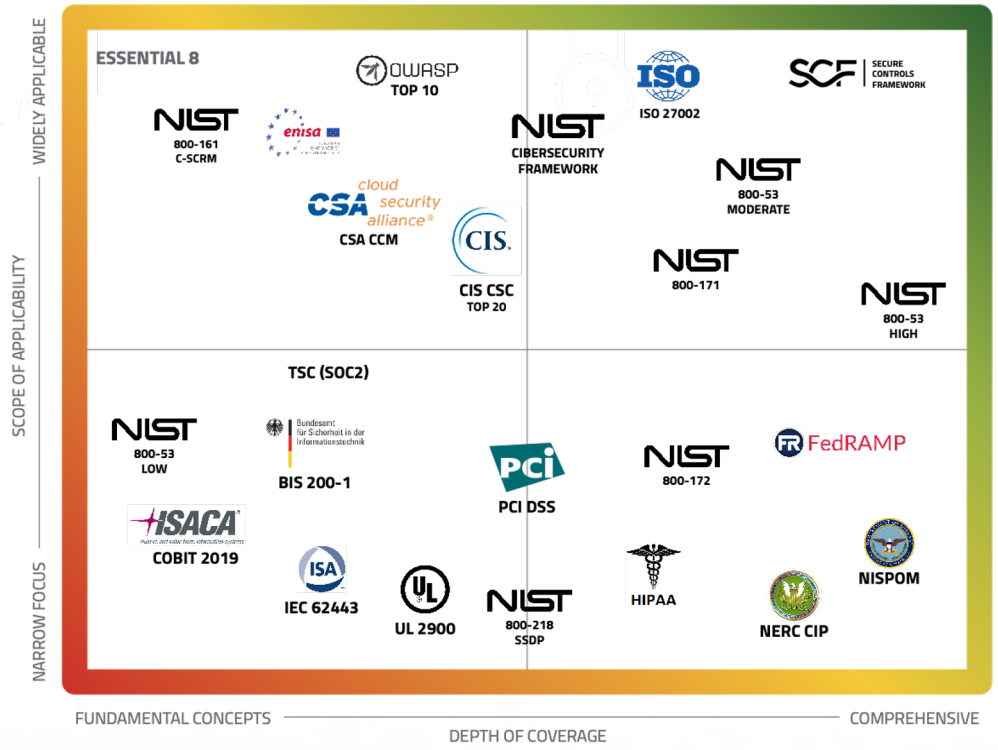
Source: CONDUSEF / SOC RADAR / Forester / Gartner

PCI Security Standards Council

Adaptive Cybersecurity Strategy

Main standards chosen in the LATAM

- Information Security Management System (ISMS)- ISO 2700 — 68%
- Control Objectives for Information and Related Technology (COBIT) — 50%
- Information Technology Infrastructure Library (ITIL) & IT Service Management (ITSM) — 43%
- Payment Card Industry Data Security Standard (PCI-DSS) — 41%
- Business Continuity Management (BCM) – ISO 22301 — 40%
- IS0 31000 & Risk Management NIST Standard — 28%
- Sarbanes Oxley [SOX] Committee of Sponsoring — 24%
- Organizations of the Treadway Commission (COSO) Framework — 23%

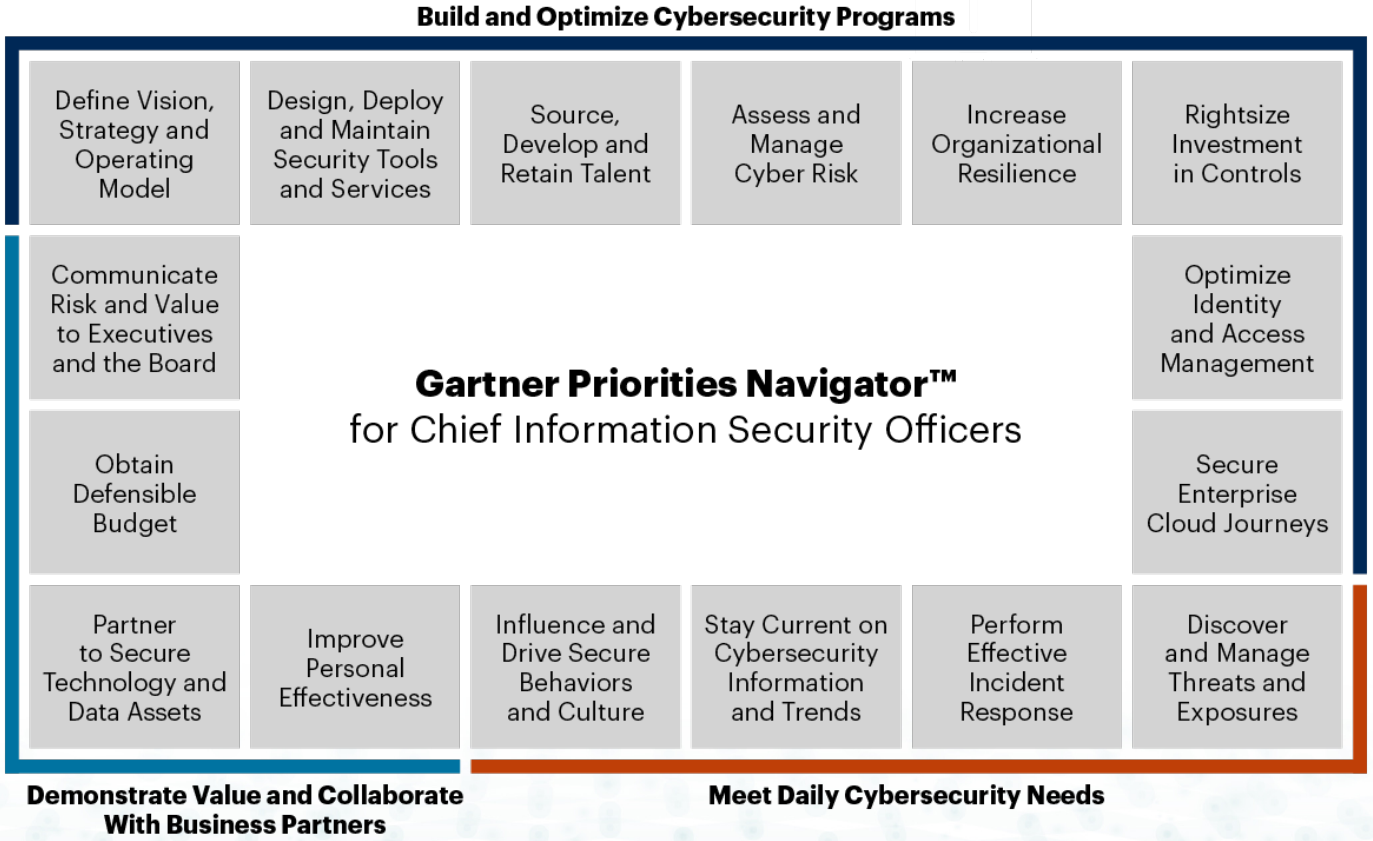


Source: SG/OEA based on information collected from banking entities in Latin America and the Caribbean.

PCI Security Standards Council®

Adaptive Cybersecurity Strategy

Delivering effective cybersecurity initiatives helps cybersecurity leaders balance the dual role of protecting the organization and delivering business value in constantly shifting threat and operating environments.

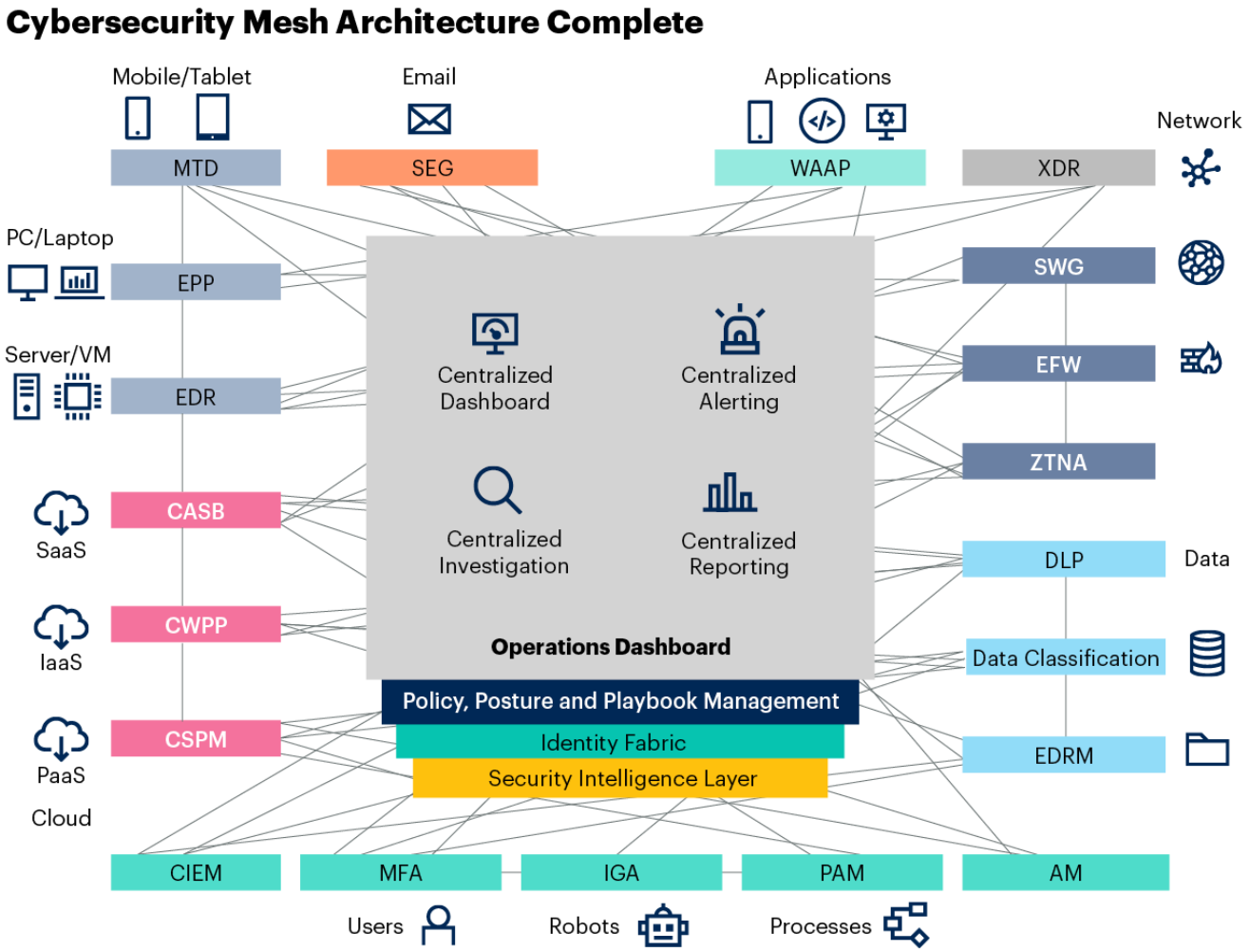


Source: Gartner
802579_C

PCI Security Standards Council

Gartner

Adaptive Cybersecurity Strategy



Source: Gartner
754315_C

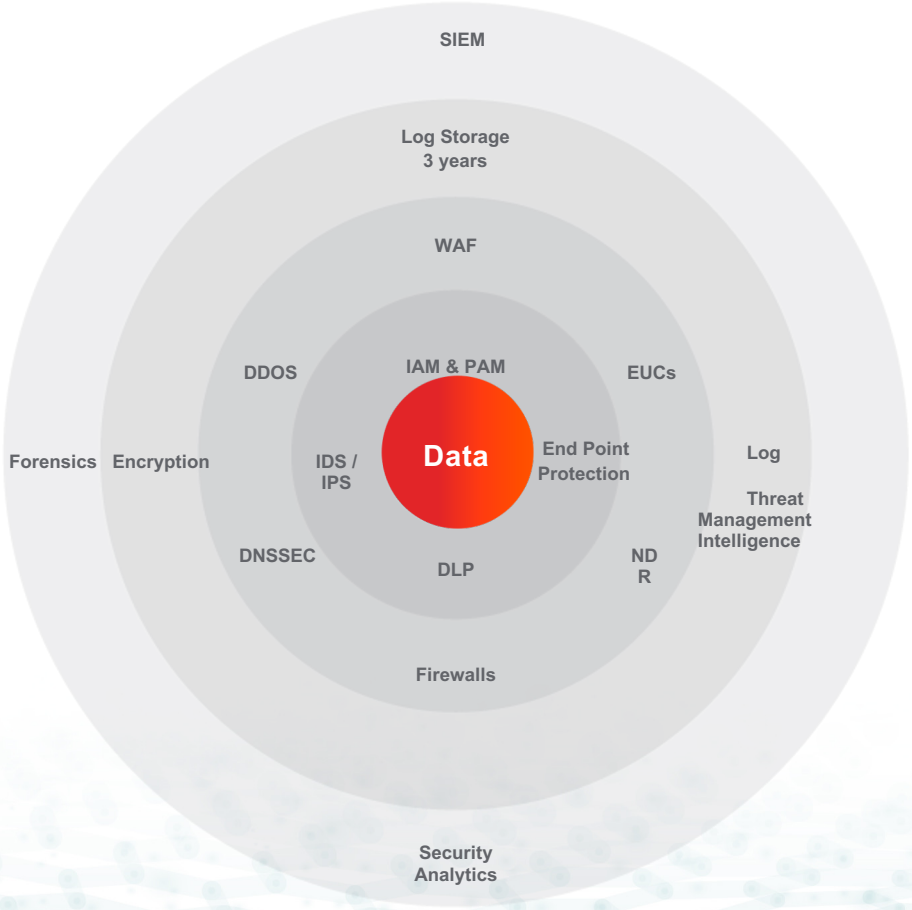
PCI Security Standards Council

Gartner

Key Takeaways

Organizations adopt a cybersecurity mesh architecture that includes AI, and combining the listed approaches will help them reduce the likelihood of a cybersecurity incident materializing.

1. Investment in the development of human capabilities.
2. Establishment of a Voluntary RMF or Standards.
3. Strategic Investment in:
    - Infrastructure and Cybersecurity Technologies
    - Artificial Intelligence applied to cyber defense.
4. Strategic cloud adoption.
5. Implement Identity governance and access management.
6. Improve Monitoring, detection, and automated response.
7. Improve Visibility, data analytics, and machine learning.
8. Adoption of a zero-trust philosophy.



Fuente: The Future of Security Architecture:
Cybersecurity Mesh Architecture (CSMA), 21 June 2023 - ID G00754315

PCI Security Standards Council

Key Takeaways

Cybersecurity in the financial sector goes beyond complying with regulations; it is an **ethical commitment** to the patrimonial protection of our information assets, which, for our clients, cements trust in our institutions. It demands a proactive stance, perfecting security processes, protection, and sustained investment in **technology** and **human talent**.

Valther Galván Ponce de León
CISO

Thank you

PCI Security Standards Council