Google Cloud Whitepaper
September 2023

Telecoms Regulatory Themes in Latin America

Telecoms Regulatory Themes in Latin America

Introduction **2**
Regulatory themes **3**
Foundational security 3
Data privacy and communications confidentiality 4
Data residency 5
Operational requirements 5
Google Cloud security solutions **6**
Security Foundations solution 6
Security and Resilience Framework (SRF) solution 6
Web App and API Protection (WAAP) solution 7
Autonomic Security Operations (ASO) solution 7
Conclusion **7**

Disclaimer

This whitepaper applies to Google Cloud products described in the Google Cloud Services Summary. The content contained herein is correct as of September 2023 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

Telecommunications is perhaps the most significant engine of world economic growth. Telecoms have powered social change and business expansion for almost 200 years, from telegraphs at the dawn of the Industrial Revolution to today's mobile apps, video, and data services. This does not show any signs of slowing down as mobile data consumption is set to quadruple between 2021 and 2027[1] in Latin America, accounting for 83% of all connections. It's easy to see why: Communications Service Providers (CSPs), as they are known today, connect people and their inventions, enabling new markets and innovations.

Accordingly, the leaders of CSPs are looking for innovative ways to unlock new revenue streams, transform the end-to-end customer experience, handle explosive usage, effectively manage increasingly complex systems, unlock the full potential of their data, and deliver on sustainability objectives.

Underpinning these focus areas, CSPs in Latin America are focused on ensuring they operate their critical infrastructure in line with ever-evolving regulatory, security, data privacy, and sovereignty requirements. As organizations accelerate their digital transformation journeys towards long-term growth - powered by cloud technology - there is a need to understand both the implications of these regulations for cloud and how the cloud can help CSPs to address these challenges.

This paper provides:

- Insight into the key themes and principles that emerge from telecoms and security-related regulations, guidelines, and standards that apply across Latin America
- Guidance on how Google Cloud can help CSPs meet their regulatory requirements

Regulatory themes

Telecom networks are critical to supporting economic development and national security across Latin America. CSPs are also trusted with large amounts of sensitive customer information. Therefore, CSPs and the telecommunication networks that they operate are subject to many security and privacy-related regulations. In the context of Latin America, this includes both global security standards and national-level regulation and guidelines.

In this section, we summarize the main themes emerging from these regulations and how Google Cloud can help.

[1] GSMA, 2022

Foundational security

CSPs are high-profile targets for cybersecurity attacks and require protection against cybersecurity risks that include state-sponsored attacks, advanced persistent threats sponsored by nation states, insider threats, and industrial espionage. Increasing cybersecurity concerns have led governments and organizations to work together to shape cybersecurity requirements and frameworks, including global standards such as:

- ISO 27001
- ISO 27017,
- ISO 27018
- AICPA SOC2 (SSAE 18)

Security regulations and guidelines identify specific security measures and best practices across domains, such as physical security, network security, identity and access management, security incident management, and personnel security.

How we help: Google Cloud has comprehensive and in-depth security controls that we have deployed to help protect your data, summarized in this security overview paper. Other papers detail our security practices in specific areas, such as encryption at rest, encryption in transit, and infrastructure security. Google Cloud also publishes guidance on security best practices, use cases, and blueprints.

Google Cloud's security, third-party audits, and certifications help support customer's compliance. Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google Cloud undergoes several independent third-party audits regularly to provide this assurance. Customers can request reports via our Compliance Reports Manager.

Data privacy and communications confidentiality

With consumers entrusting CSPs with large volumes of sensitive customer data, including personally identifiable information and communications records, it's important that the consequences of data breaches are understood.

Protecting customer data privacy and confidentiality of communications are fundamental requirements for telecom operators. Unethical usage of customer data can lead to financial penalties and loss of customer trust.

How we help: Google Cloud's trust principles provide a starting point for our approach to data privacy.

Customers own their data, not Google. We want you to feel confident that taking advantage of Google Cloud doesn't require you to compromise on security or control of your business's data. Google Cloud does not use customer data for advertising and we do not sell customer data to third parties. Our Cloud Data Processing Addendum for Google Cloud further describes our commitment to protecting your data.

Google Cloud is also compliant with international standards on data privacy, such as:

- ISO 27018 (Cloud Privacy)
- ISO 27701 (Privacy - Data Processor)

Additionally, Access Transparency for Google Cloud and Google Workspace supports this trust by providing logs of actions taken by Google staff and the reason for access including references to support tickets where relevant.

For more information, refer to our whitepaper on trusting Google Cloud with your data and to Google Cloud's Privacy Resource Center.

Data residency

The regulatory bodies of Latin American states expect organizations to know where customer data resides. To meet their data residency needs, CSPs in Latin America look to cloud providers to offer the same level of trust and transparency that their customers demand.

How we help: Google Cloud services offer customers the ability to control where your data is stored via Data Residency. Google will store that customer data at rest only in the selected Region/Multi-Region in accordance with our Service Specific Terms.

In Latin America, customers can store data at rest exclusively within two cloud regions, Santiago Region Data Center (southamerica-west1) and São Paulo Region Data Center (southamerica-east1). We have also announced plans to bring Google Cloud regions to Querétaro soon.

To assist customers in enforcing these controls, Google Cloud offers Organization Policy constraints which can be applied at the organization, folder, or project level. You can limit the physical location of a new resource with the Organization Policy Service resource locations constraint.

Google Cloud customers can use VPC Service Controls to restrict the network locations from which users can access data, defining a service perimeter outside of which customer data

cannot be accessed. This functionality allows customers to limit user access by IP address filtering, even if the user is otherwise authorized. Cloud Armor also allows customers to restrict locations from which traffic is allowed to their external load balancer.
Google Cloud customers can use VPC Service Controls to restrict the network locations from which users can access data, defining a service perimeter outside of which customer data cannot be accessed. This functionality allows customers to limit user access by IP address filtering, even if the user is otherwise authorized. Cloud Armor also allows customers to restrict locations from which traffic is allowed to their external load balancer.

Operational requirements

Should the availability of public communication services be impacted by a security incident, widespread disruption could occur. This has potential implications for both public safety and national security. CSPs could also face fines and reputational damage in addition to lost revenue. CSPs are responsible for ensuring they are designing for high availability (as well as security) when planning cloud solutions.

How we help: Google Cloud publishes architecture guidelines to help customers achieve high availability at scale.

Google Cloud also supports customers with Backup and Disaster Recovery solutions. CSPs can use these solutions to design, build, and validate robust disaster recovery patterns that meet their specific recovery time objectives (RTOs) and recovery point objectives (RPOs).

To complement this, Google Cloud also has comprehensive internal plans and systems for its business continuity (refer to ISO 22301).

Google Cloud also offers customers the choice of manual or automated software updates, with the flexibility to control software update approvals and scheduling. Refer to OS Patch Management for an example.

Google Cloud security solutions

In addition to the security features and regulatory compliance already described, Google Cloud offers several Security Solutions for a more comprehensive and holistic approach to security.

CSPs migrating to the cloud may not initially have the expertise to decide which security capabilities they need. Security solutions help customers identify those needs and rapidly roll out of relevant security functionality based on common blueprints and established best practices.

Security Foundations solution

As a starting point for customers who need clarification on their security needs, the Security Foundations solution includes a set of recommended products and security capabilities to help CSPs achieve a strong security posture within their Google Cloud environment.

This solution is based on the Security Foundations whitepaper and aligns with Google Cloud's security best practices.

Security and Resilience Framework (SRF) solution

Google Cloud can also support CSPs in carrying out a thorough review of their security practices.

The Security and Resilience Framework helps customers to establish or refresh their security program, founded on a risk-based assessment of the entire cybersecurity lifecycle (identify, protect, detect, respond, recover), using established industry frameworks.

The Discovery Platform supports the assessment and includes security maturity assessments across multiple domains. Google Cloud will provide a tailored set of recommendations around security best practices and recommended Google Cloud security products and solutions.

Web App and API Protection (WAAP) solution

The Web App and API Protection solution (WAAP) provides capabilities that protect applications, websites, and public APIs from internet-based threats, including DDOS, fraud, and botnet attacks.

This solution is relevant for all CSPs since DDOS attackers commonly target their infrastructure and systems, and unfortunately, the increased adoption of APIs by CSPs can expose their capabilities. In 2022, Google Cloud successfully identified and blocked the largest DDOS attack on record, demonstrating our ability to protect customers from internet-based attacks.

The WAAP solution includes the following products:

- Cloud Armor
- reCAPTCHA Enterprise
- Apigee API Management

Autonomic Security Operations (ASO) solution

Google Cloud's Autonomic Security Operations solution helps CSPs withstand security attacks through an adaptive, agile, and highly automated approach to threat management.

This solution is relevant for Providers that are interested in transforming their existing Security Operations Centre (SOC) or Security Incident and Event Management (SIEM) by increasing scale, automation, and the use of machine learning (ML) to keep up with a high volume of security incident data and deliver effective threat intelligence and incident response. For more information, refer to our Autonomic Security Operations whitepaper.

Finally, customers can leverage the power of Chronicle and Mandiant, to customers can transform their security operations and achieve a 10X increase in productivity, visibility and speed.

Conclusion

CSPs in Latin America are looking to transform and grow their business. Digital transformation initiatives include modernizing core network and IT systems (including operations support system (OSS) and business support system (BSS)) via migration to the cloud and adopting cloud-native architectures. CSPs are also looking to improve customer experience and operational efficiency and monetize their data by adopting cloud-based analytics and ML to gain insights from their customer and network data.

Google Cloud continues to innovate in areas such as encryption, key management, auditability, transparency, and data residency to help CSPs meet their operational security, resilience, and data privacy needs.