Information Security Strategy

At América Móvil and its subsidiaries, a preventive approach to information security has been key. It has enabled us to anticipate risks before they materialize and to identify more efficient processes and controls, always guided by a clear commitment to continuous improvement.

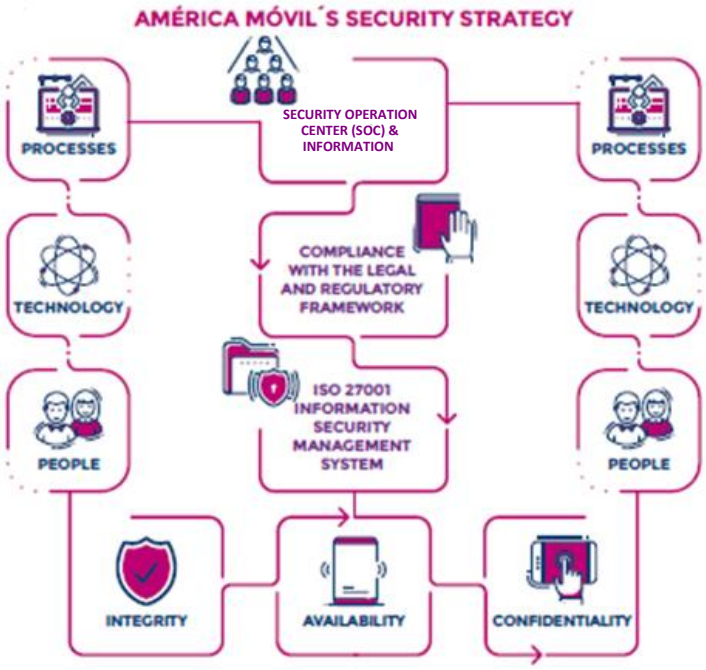
Based on a thorough risk analysis—considering both probability and impact—we developed our **Corporate Information Security Strategy**. This strategy serves as a roadmap for the corporation and its subsidiaries to mitigate existing risks and prevent their occurrence. It does so through the enhancement, creation, implementation, and testing of controls, processes, services, and tools aligned with this objective. Additionally, the strategy provides a deeper perspective that allows for more efficient budgetary investments.

Cyberattacks, theft of **sensitive information**, and increasingly sophisticated forms of cybercrime represent significant risks for organizations worldwide. These threats can severely impact both corporate reputation and financial stability, affecting companies and their clients alike.

At América Móvil, we offer cybersecurity connectivity solutions that not only provide users with a sense of safety but also contribute to the broader information security of the communities in which we operate.

Our comprehensive security strategy encompasses cybersecurity, data privacy, and communications protection, and is built upon three core pillars:

- **Integrity:** Personal information must remain complete and accurate, for which we have established appropriate measures.
- **Availability:** Information must be available to its owners or authorized users at the precise moment they need it.
- **Confidentiality:** Personal data will be used exclusively by authorized personnel who have the necessary justification to use it.



Through our Information Security Strategy, we efficiently manage and safeguard financial and confidential information, while minimizing the risks of illegal or unauthorized access.

At América Móvil, we have developed an **Information Security Regulatory Framework** composed of 12 domains. These domains encompass the minimum policies and procedures that must be considered in the operations of our subsidiaries. Compliance and execution are overseen by the Information Security Officers and Information Security Committees at both the Corporate and subsidiary levels, supported by a **Global Security Operations Center (SOC)** managed by Scitum, a Telmex subsidiary. This SOC includes a cyber intelligence team dedicated to identifying and responding to threats.

The **SOC** plays a dual role: securing all our operations to instill confidence in our services and solutions, and providing cybersecurity products and advisory services to our corporate clients to help them proactively address emerging challenges.

Our personnel play a critical role in the success of our Information Security Strategy. For this reason, we **provide ongoing training** on our security policies and procedures. We also regularly conduct awareness campaigns and simulated phishing exercises to reinforce best practices and controls related to system access and the handling of sensitive information across the Company and its subsidiaries.

To stay aligned with the latest trends, we host the **"América Móvil Cybersecurity Symposium"** at least once a year. This event covers key topics such as information security trends, the Internet of

Things, standards, challenges, opportunities, digital transformation, and access controls, among others.

We continuously evaluate and update our Information Security Strategy, guided by principles of prevention, continuous improvement, and the sharing of best practices across all companies within the Group.

INFORMATION SECURITY GOVERNANCE

Our Chief Information Security Officers (CISOs) lead the company-wide efforts to ensure the effective implementation of our Information Security Strategy and alignment with ISO 27001 certification across all operations.

We also have a **Corporate Information Security Committee** that meets twice a month to oversee the implementation of América Móvil's Information Security Strategy. Its key responsibilities include:

- Identifying major business risks related to operations, services, and the technological environment.
- Developing and managing the security strategy through the creation and monitoring of the Strategic Information Security Plan.
- Managing and allocating both corporate and local budgets for information security.
- Defining priority actions in response to current and emerging threats.

Our updated governance structure enables close coordination between the information security teams of our subsidiaries and Scitum personnel for effective incident detection and response. We also maintain a robust communication mechanism across operations to ensure timely alerting and response.

Local Information Security Officers are responsible for:

- Adopting and implementing information security policies and procedures.
- Establishing strategies to enhance the confidentiality, integrity, and availability of information assets.
- Deploying mechanisms aligned with best practices to protect information resources.
- Coordinating the evaluation and execution of projects supporting information security activities.
- Overseeing communication plans and awareness campaigns.
- Analyzing security incidents to identify solutions and preventive measures.
- Assessing new and existing infrastructure that supports critical business processes.
- Leading the local Information Security Committees within each subsidiary.
- Monitoring improvement actions related to reported incidents.
- Supporting other departments in complying with information security guidelines.

- Ensuring that all efforts, resources, tools, controls, and monitoring activities are aligned with the assurance of information availability, integrity, and confidentiality.

Reporting any incident that could compromise critical information—including its potential impact and mitigation plans—to the local CEO, the CISO, and the Corporate Information Security Committee.

Each subsidiary also has its own Local Information Security Committee. These interdisciplinary committees include representatives from various departments (such as IT, engineering, finance, operations, and maintenance) and are chaired by the local Information Security Heads. Additionally, each operation designates a senior executive responsible for reviewing the Cybersecurity Strategy. Every country develops a Strategic Information Security Plan, which is reviewed and updated annually or semi-annually.